MorphoManager

User Manual

SAFRAN
Morpho

Contents

Introduction 5
Support 5
Overview 6
What is a client? 6
What is a server? 6
What is a fingerprint enrollment device? 6
What is a Biometric Device? 7
Setting up MorphoManager 8
Computer hardware requirements: 8
Supported Operating Systems: 8
Installation of MorphoManager software 8
Setting up MorphoManager on a single PC 9
Server and Client Installation 10
Product Registration 11
Procedure for registration 11
Activate Online 12
Activate Offline 13
Advanced Client Configuration 15
Advanced Server Configuration 17
Server Manager 19
Running MorphoManager Login 19
Home Screen 20
Administration 21
Operators 21
Creating a new Operator 21
Screen 1 – Operator Details 21
Screen 2 – Operator Roles 22
Biometric Device Profile 23
Creating a new Biometric Device Profile (Express) 23
Screen 1 – Configuration Details 23
Screen 2 – Biometric Threshold Settings 24
Screen 3 - Multi-Factor Mode Settings 25
Screen 4 – Access Control Mode Setttings 26
Screen 5 – Function Key Mode for MA 100, J, 500, and VP Family 27
Screen 6 – MorphoAccess SIGMA Settings 28
Screen 7 – MorphoAccess Sigma Key Mode Settings 29
Screen 8 – Morpho 3D Face Settings 29
Screen 9 – Video Phone Server Settings 30
Creating a new Biometric Device Profile (Advanced) 31
Screen 2- Advanced Parameters for MorphoAccess 100, 500, J, and VP 31
Screen 3 – Advanced Parameters for MorphoAccess SIGMA 31
Creating a new Biometric Device Profile (External) 32
Biometric Device 32
Create a Biometric Device 32
Modify a Biometric Device 34
Delete a Biometric Device 34
Biometric Device Status and Tasks 34
Troubleshooting and Maintenance 35
Toolbar Functionality 35
Wiegand Profiles 36
Create a Wiegand Profile 36
Screen 1 – Configuration Details 36
Screen 2 – Wiegand Profile Elements 36
User Policy 38
Create a new User Policy 38
Screen 1 – Details 38
Screen 2 – Time Mask 40

© Refer to End User License Agreement for Copyright Notice

User Distribution Group 40
Create a User Distribution Group 40
Screen 1 – Details 40
Screen 2 – Select Biometric Device Access 41
Screen 3 – Select MorphoManager Client Access 41
User Authentication Mode 41
Create a new User Authentication Mode 42
Screen 1 – Details, MA 2G Family Mode, and 3D Face Mode 42
Screen 2 – Details for MA Sigma mode 44
Operator Role 45
Clients 46
Scheduled Reports 49
Card Template 51
Card Encoding Log 52
Event Logs 52
Exception Logs 53
System Configuration 53
Section 1 – Time and Attendance 53
Section 2 – Contactless Keys 54
Section 3 – Communications Engine 54
Section 4 – System Functionality 55
Section 5 – Automatic Log Management 56
Section 6 – Gateways 56
Section 7 – Connector Service 56
Section 8 – BioBridge 57
Section 9 - Privacy Mode 58
User Management 59
Creation and enrollment of a User 59
Screen 1 – User Details 60
Screen 2 – Additional Details 61
Screen 3 – Contact Details 61
Screen 4 – Biometric Device Override Details (If a Wiegand Profile is set) 62
Screen 5 – User Distribution Groups 62
Screen 6 – Morpho 3D Face Reader Override Details 62
Screen 7 – MSO Identification Client Override Details 63
Screen 8 – Photo Capture 63
Screen 9 – PIN Code 64
Screen 10 – Fingerprint Capture 65
User Actions 69
Filtering 70
MSO Identification 70
Biometric Device Profile Creation Tool 72
Onsite/Offsite 72
Access Logs 73
Reports 74
User Activity Report 74
Biometric Device Activity Report 75
User Policy Activity Report 75
All Activity (included all users and Biometric Device) 75
Inactivity Report 75
List Report 75
User Policy Members Report 75
Permissible Report 75
Database Management 76
Database Backup Tool 76
Database Copy Tool 76
Copying a database 76
Biometric Device Setup 79
Biometric Device IP Address Configuration 79
Biometric Device Wiring 80
MA 500 / MA 500+ Series: New Block board wiring 80

© Refer to End User License Agreement for Copyright Notice

MA 500 Series: Old block board wiring 81
Ethernet Interface (LAN 10 Mbps) 82
T568B and T568A RJ45 Wire Positions 82
Biometric Device TCP\IP Ethernet Wiring 83
Power Supply source 83
Wiegand output wiring 84
Wiegand input wiring 84
Output relay and Tamper-Switch 84

© Refer to End User License Agreement for Copyright Notice

Introduction

MorphoManager is the latest generation of biometrically powered Access Control and Time & Attendance capture software. The software works with Biometric Device hardware to capture user's finger prints, photos, and personal details. The fingerprint information is sent to specified Biometric Devices where access control is required and where users clock on and off throughout the day. MorphoManager also works with Morpho 3D Face Readers to capture user's facial traits.

Support

Please contact your installer for support.

© Refer to End User License Agreement for Copyright Notice

Overview

A MorphoManager system consists of four components:

- A MorphoManager Server
- At least one MorphoManager Client
- A fingerprint/finger vein/3D Face enrollment device.
- At least one Biometric Device.

What is a client?

A client is a computer that has the **MorphoManager Client** software installed. There can be more than one client in a MorphoManager system.

The client application provides the management of access points, enrolling of personnel, and reporting. A PC that has the enrollment scanner connected and is used as the user registration PC. A client PC may be used to view data and not have an enrollment device connected.

What is a server?

A server is a computer that has the **MorphoManager Server** software installed.

The server manages the communication between the Biometric Device and the PC and interacts with the database. It also handles requests from clients.

What is a fingerprint enrollment device?

A fingerprint enrollment device captures an image of a user's fingerprint, extracts the features and sends it to the MorphoManager software. This information is sent to a Biometric Device for user authentication. There are currently three types of fingerprint enrollment devices:

MorphoSmart 300
USB Fingerprint Reader

MorphoSmart 1300
USB Fingerprint Reader

MorphoSmart FVP
USB Fingerprint and Vein Reader

© Refer to End User License Agreement for Copyright Notice

The readers are connected to a computer that is running MorphoManager Client software. All enrollment of personnel is performed using MorphoManager software. Device drivers for this hardware are automatically installed when MorphoManager Client software is installed.

What is a Biometric Device?

MorphoAccess 500+
(MA 500+)

MorphoAccess OMA 520
(OMA 520)

MorphoAccess VP
(MA-VP)

MorphoAccess Sigma
(MA-Sigma)

A Biometric Device such as the MorphoAccess units above are used to authenticate users and allow access to doors. They record a log of every presentation. MorphoManager is used to manage user's access to a Biometric Device.

Morpho 3D Face Reader

Like the Biometric Device devices, a Morpho 3D Face Reader is a Biometric Device used to authenticate users while recording a log of every presentation. While they are also managed by MorphoManager, they follow a different method when authenticating users.

© Refer to End User License Agreement for Copyright Notice

Setting up MorphoManager

This section outlines the requirements for MorphoManager systems.

Computer hardware requirements:

Processor:	Dual Core CPU
RAM:	4 GB
Ports:	Three USB ports
Network:	100Mbs Ethernet port required for client/server connections.
Internet Access:	Required for updates. (If no internet access is available, updates can be installed via USB memory stick or CD Rom)

Supported Operating Systems:

- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista SP1
- Microsoft Windows XP SP3
- Windows Server 2003 R2
- Windows Server 2003 R2 SP2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Installation of MorphoManager software

The installation CD contains both the client and server software.

There are two configurations for MorphoManager:

- Client and Server on the same PC

  A PC can have both the client and server software installed. The server software needs to be installed first.

- Server PC and Client PCs

  The server software needs to be installed on the server PC and the client software needs to be installed on each client PC that will connect to the server PC over a LAN or VPN connection. **The server software needs to be installed first**.

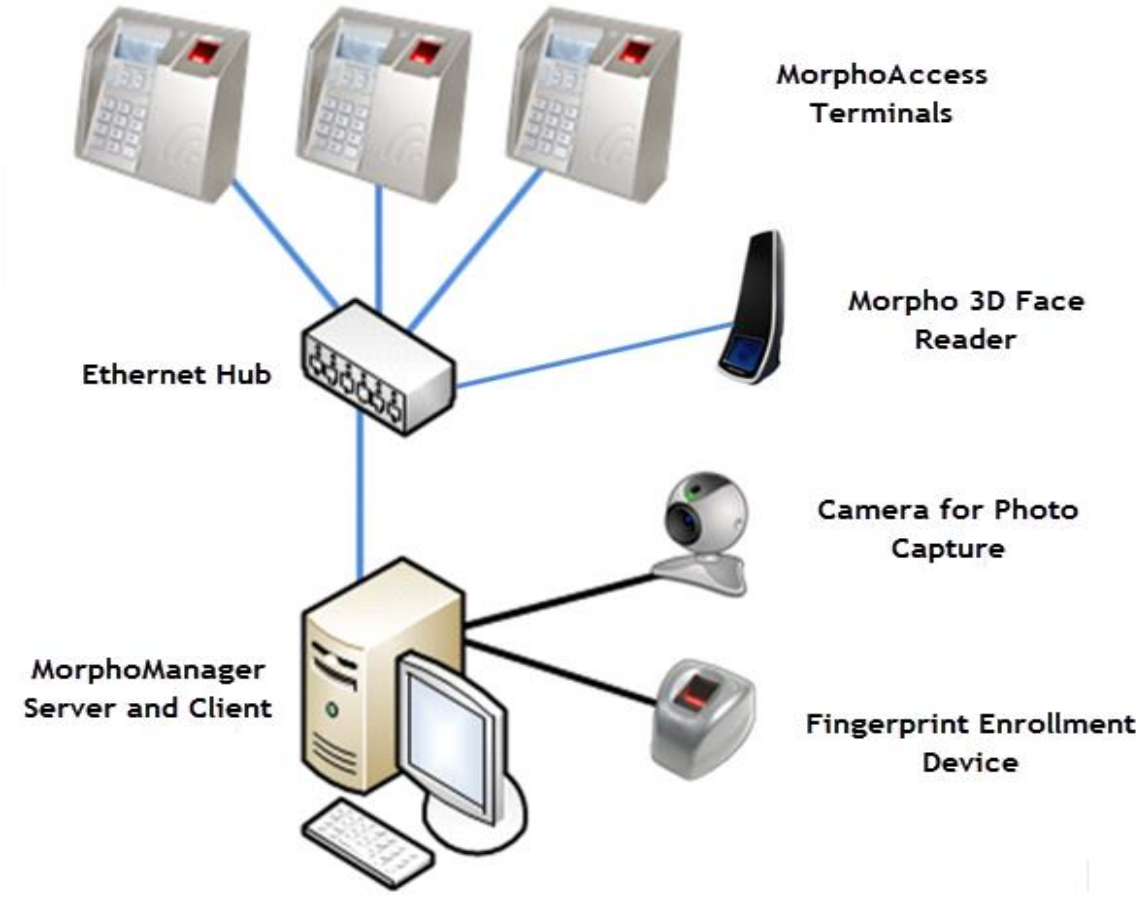
Updates for MorphoManager can be obtained by visiting: http://support.morphomanager.com/

© Refer to End User License Agreement for Copyright Notice

Setting up MorphoManager on a single PC

Both the client and the server applications can be installed on one computer.

- Load the MorphoManager CD and select the Server install.
- After the server is installed, install the client.
- Connect the MSO 300 enrollment device to the PC.
- Ensure the Biometric Devices are on the same network as the MorphoManager Server/Client PC and are in the same IP range.
- Start MorphoManager – double click on the icon on the desktop.
- When logging in for the first time the following details are used.
    - Username: **administrator**
    - Password: **password**
- It is recommended the Administrator password is changed immediately. This can be done by clicking on the **Change Password** icon on the status bar.



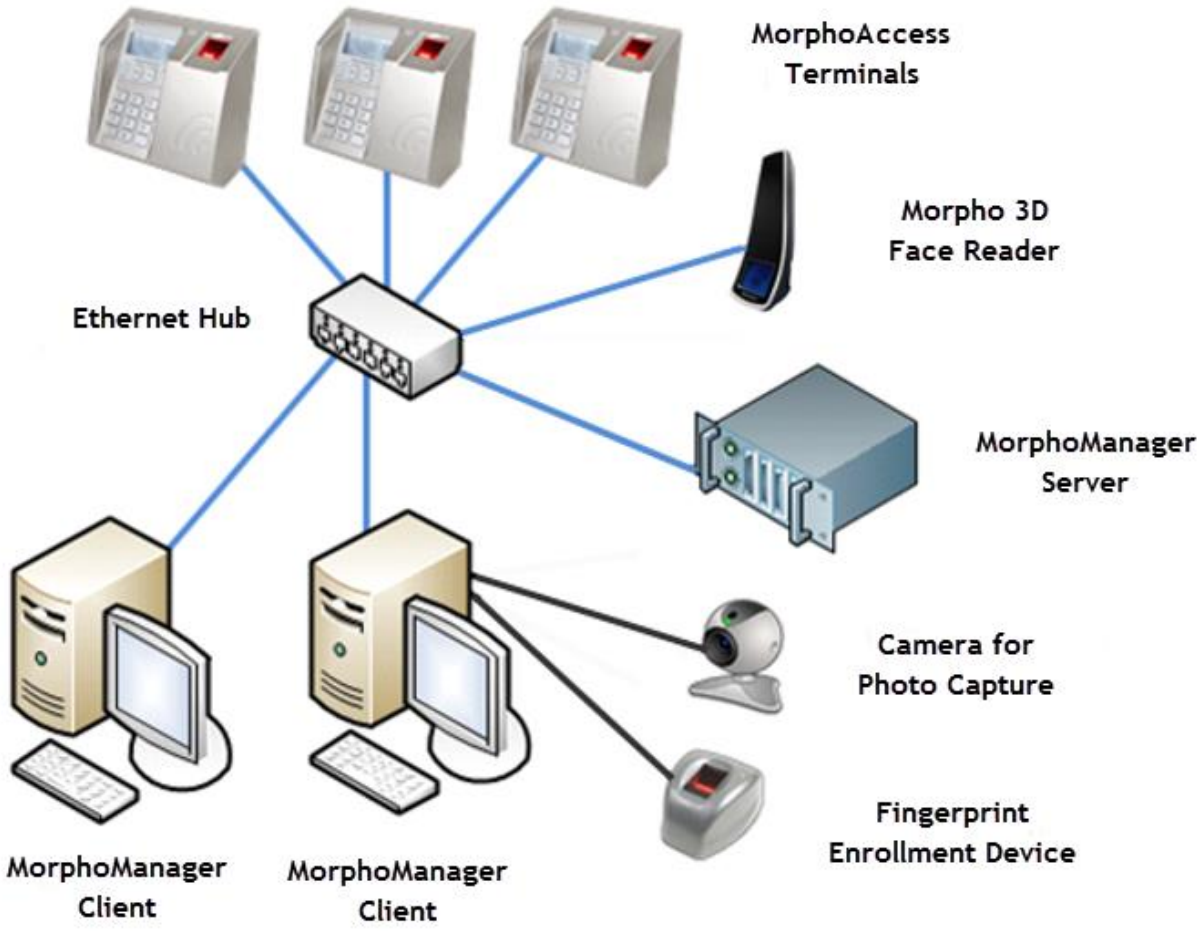
For added security, many businesses and departments have chosen to dedicate a PC for MorphoManager and often use a dedicated hub to which only the MorphoManager PC's and Biometric Devices connected.

© Refer to End User License Agreement for Copyright Notice

Alternatively, an existing hub can be used, but it is recommended that the IP range of the MorphoManager PC and Biometric Devices are different from the corporate PC's.

Server and Client Installation

This configuration can be used with an existing corporate network that already has a server. The MorphoManager client application can be installed on any PC that is attached to the server.

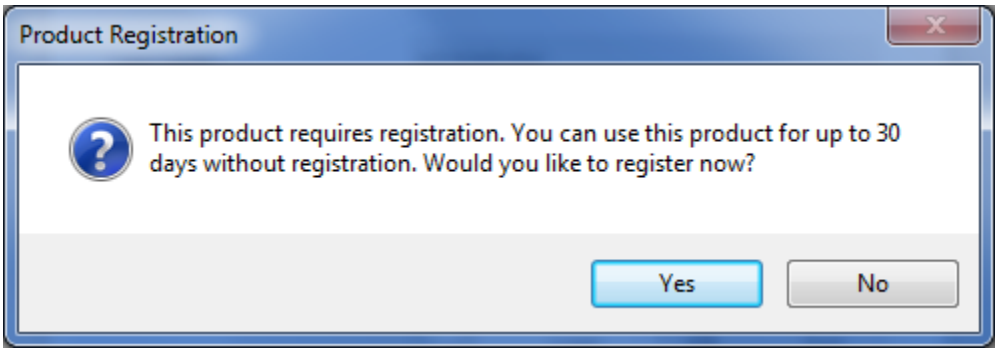


The MorphoManager server application can be installed on a separate PC which may or may not be a dedicated server.

© Refer to End User License Agreement for Copyright Notice

Product Registration

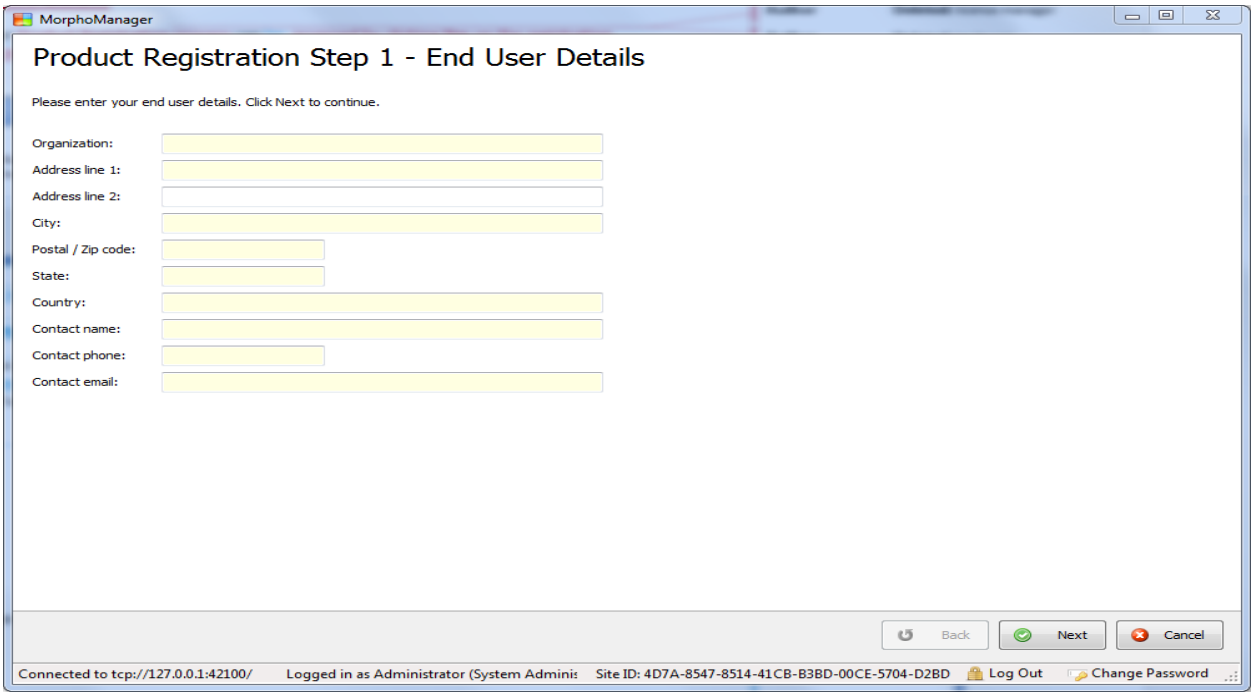
The MorphoManager Product Registration process can be accessed by clicking **Yes** on the registration prompt after logging into Morpho Manager.



If the product is not registered, MorphoManager will run for 30 days in trial mode.

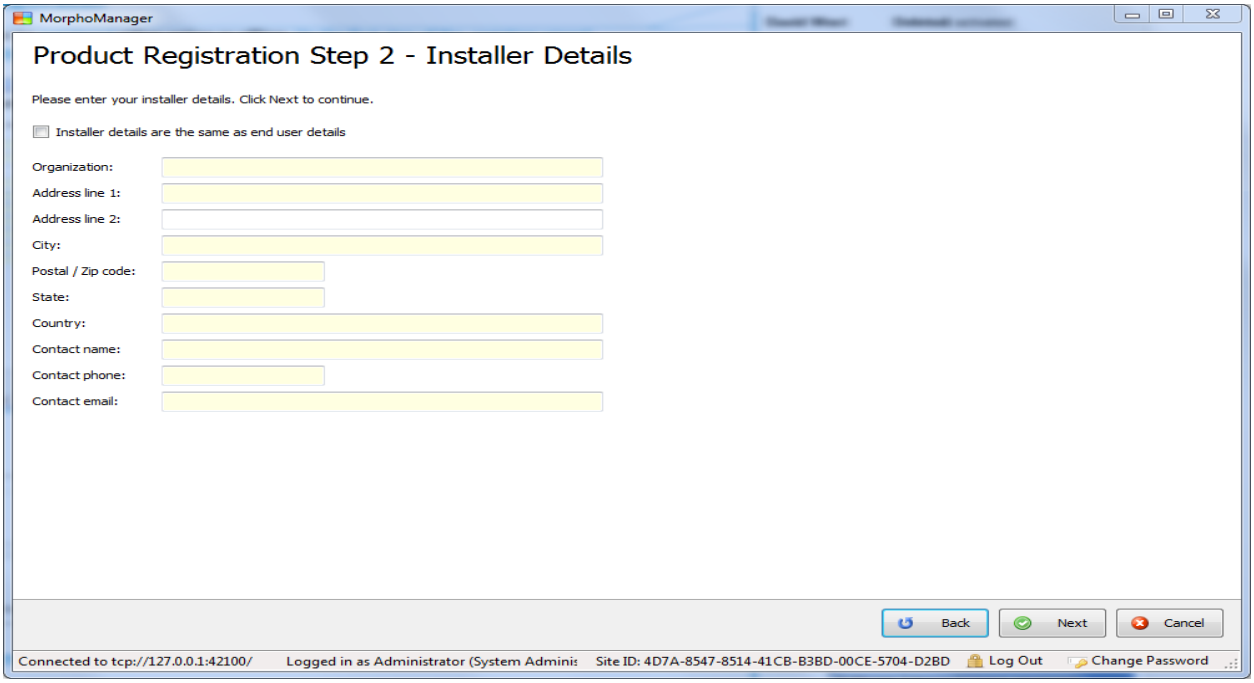
Procedure for registration

MorphoManager can be registered either online or offline. On the first step of the registration wizard enter the end user details and click **Next**.



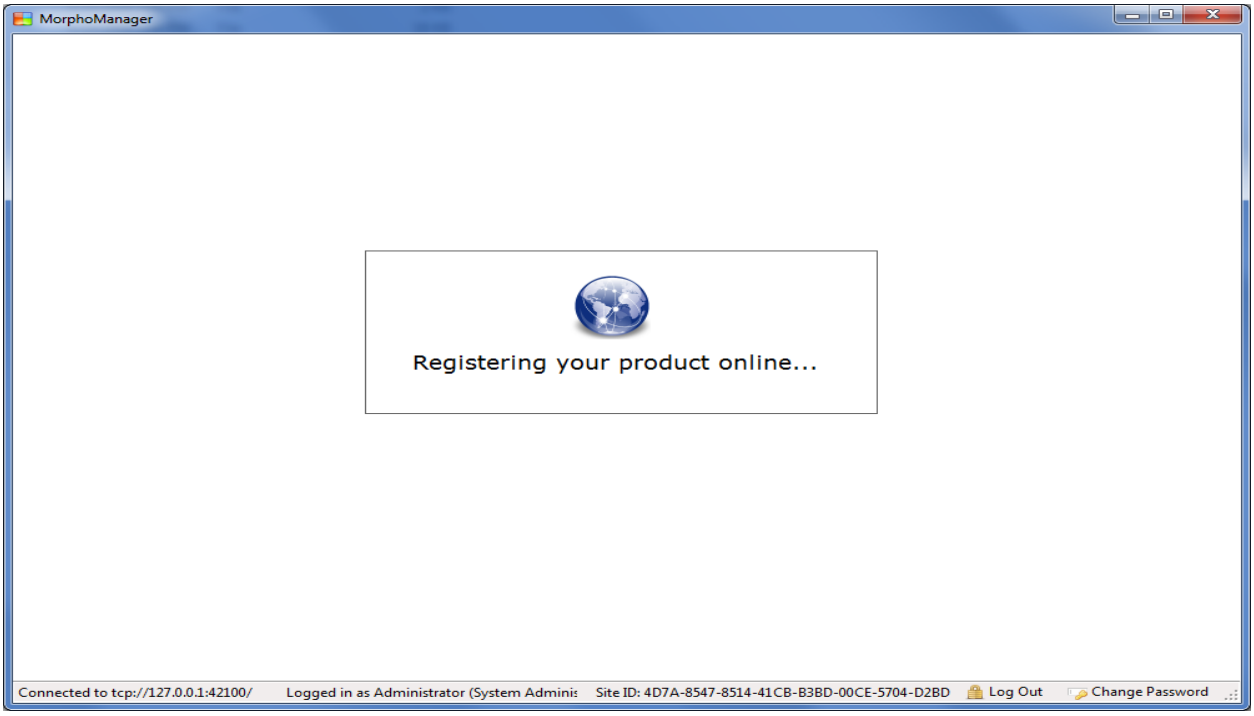
On the following screen enter the installer details and click **Next**.

© Refer to End User License Agreement for Copyright Notice



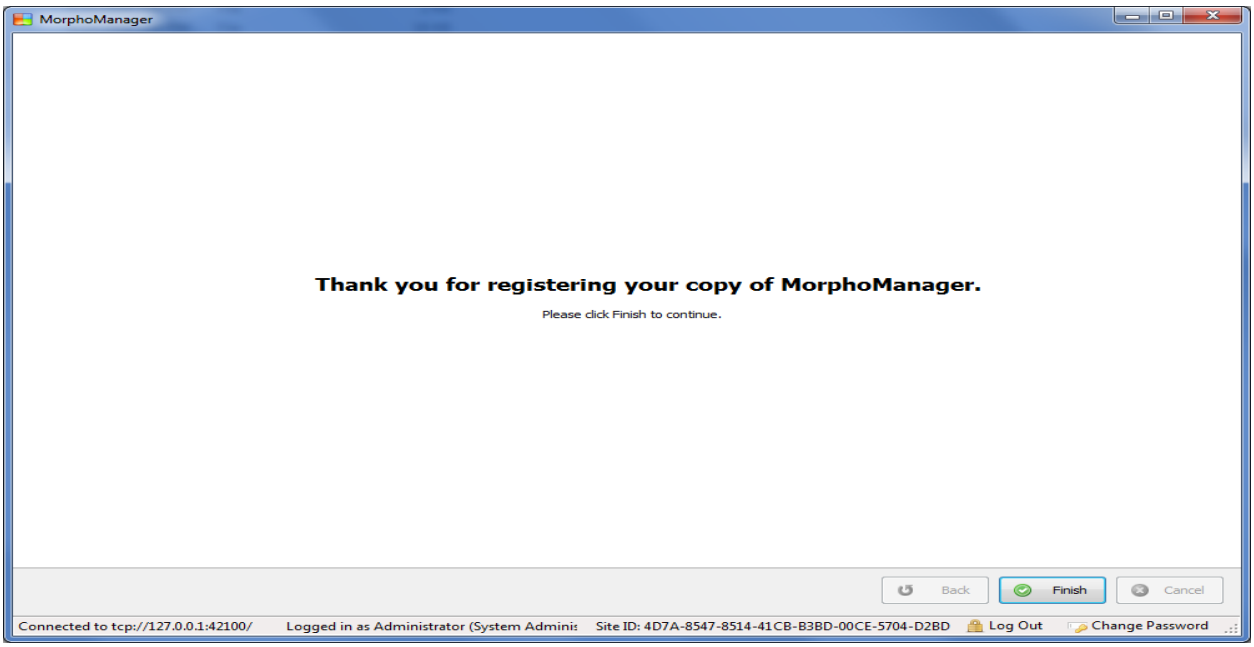
Activate Online

If you are connected to the internet you will be activated online after clicking **Next** on the Step 2 wizard screen. The following screen should appear:



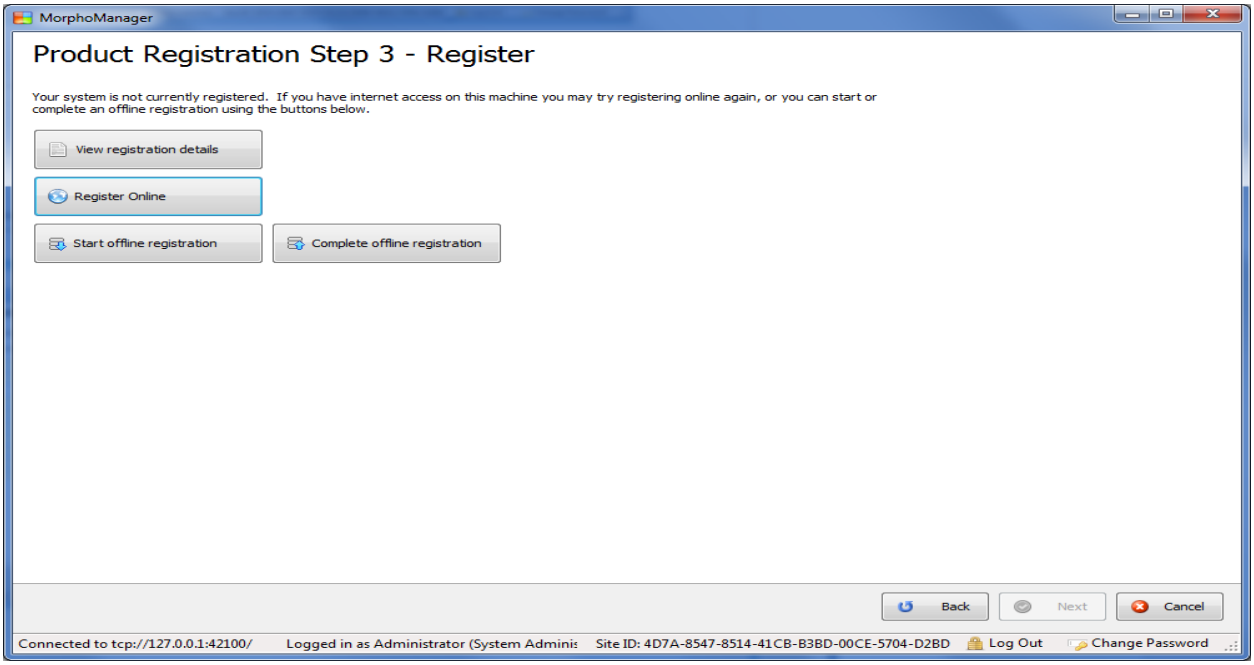
© Refer to End User License Agreement for Copyright Notice

When the process is complete the following screen will appear. Morpho Manager is now registered. After clicking **Finish** you will be taken to the MorphoManager Home Screen.



Activate Offline

If you do not have the internet, you will be shown the following screen after Step 2 mentioned in the beginning of this registration section. From here you can click **Start offline registration**.



© Refer to End User License Agreement for Copyright Notice

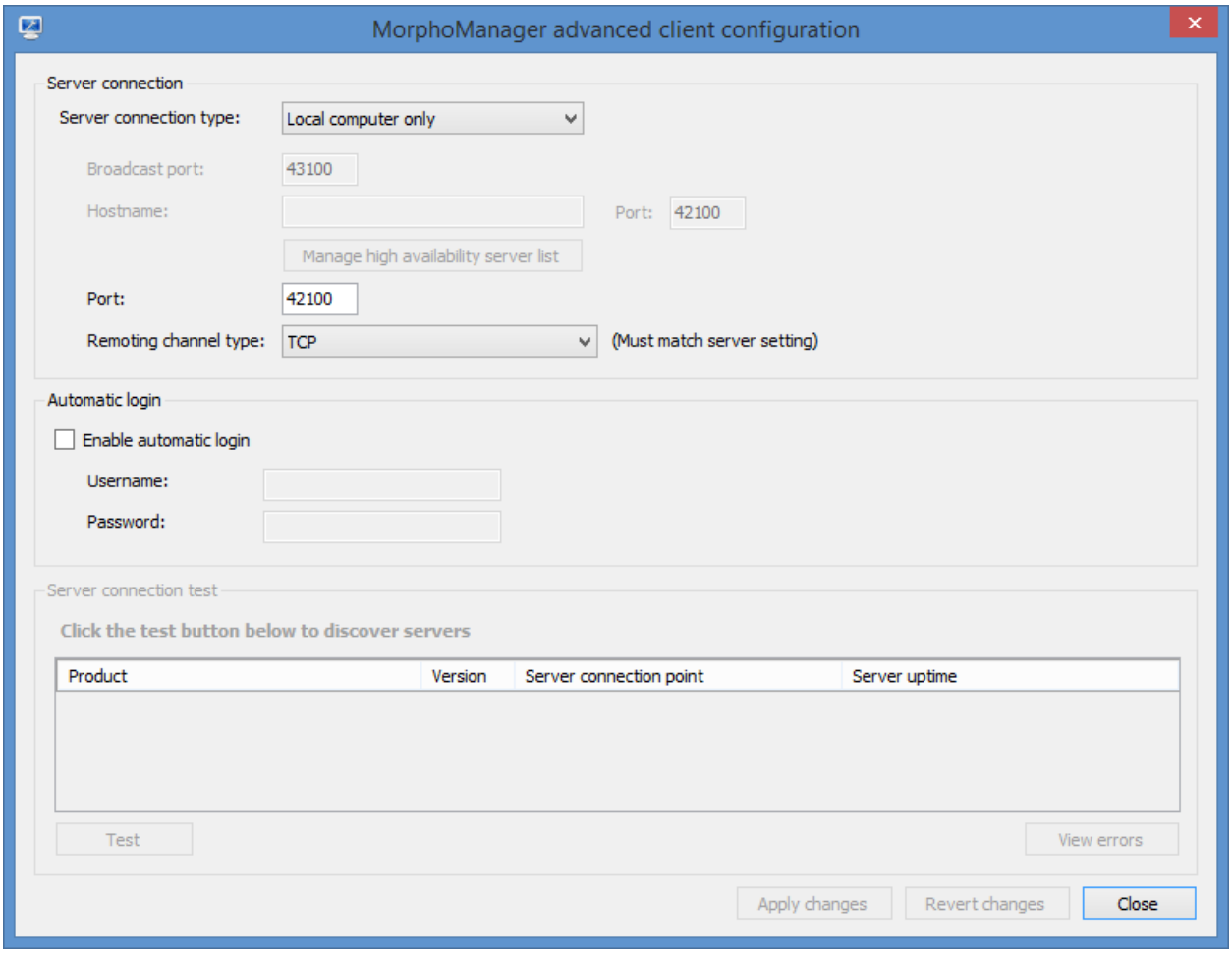
The system will prompt you to save a registration file. Choose a location, give the file a name, and click **Save**.

In the Americas email the file for registration processing to cscenter@morpho.com. For the rest of the world, please email the file to hotline.biometrics@morpho.com. Once it has been completed it will be emailed back to you. Save it where it is accessible to MorphoManager and reopen the registration process by clicking **Yes** to the registration prompt you receive when logging in to MorphoManager. You can now click the **Complete offline registration** button. Find the file and click **Open**. This will complete the offline registration process.

© Refer to End User License Agreement for Copyright Notice

Advanced Client Configuration

The MorphoManager **Advanced Client Configuration** can be found by clicking on the start menu, then selecting “MorphoManager” and then “MorphoManager Advanced Client Configuration”.



Server Connection Type:

Local Computer Only:	Use this setting when the client and server are installed on the same PC.
Manually Specified:	The server is installed on a different PC to the client. Enter the hostname or IP address of the server in the hostname box. The port must be the same as the remoting port specified on the server configuration. The port values should only be changed if the default ports are being used by another application.
Automatic Discovery:	Used when the server is installed on a different PC to the client. The application will attempt to automatically find a MorphoManager

© Refer to End User License Agreement for Copyright Notice

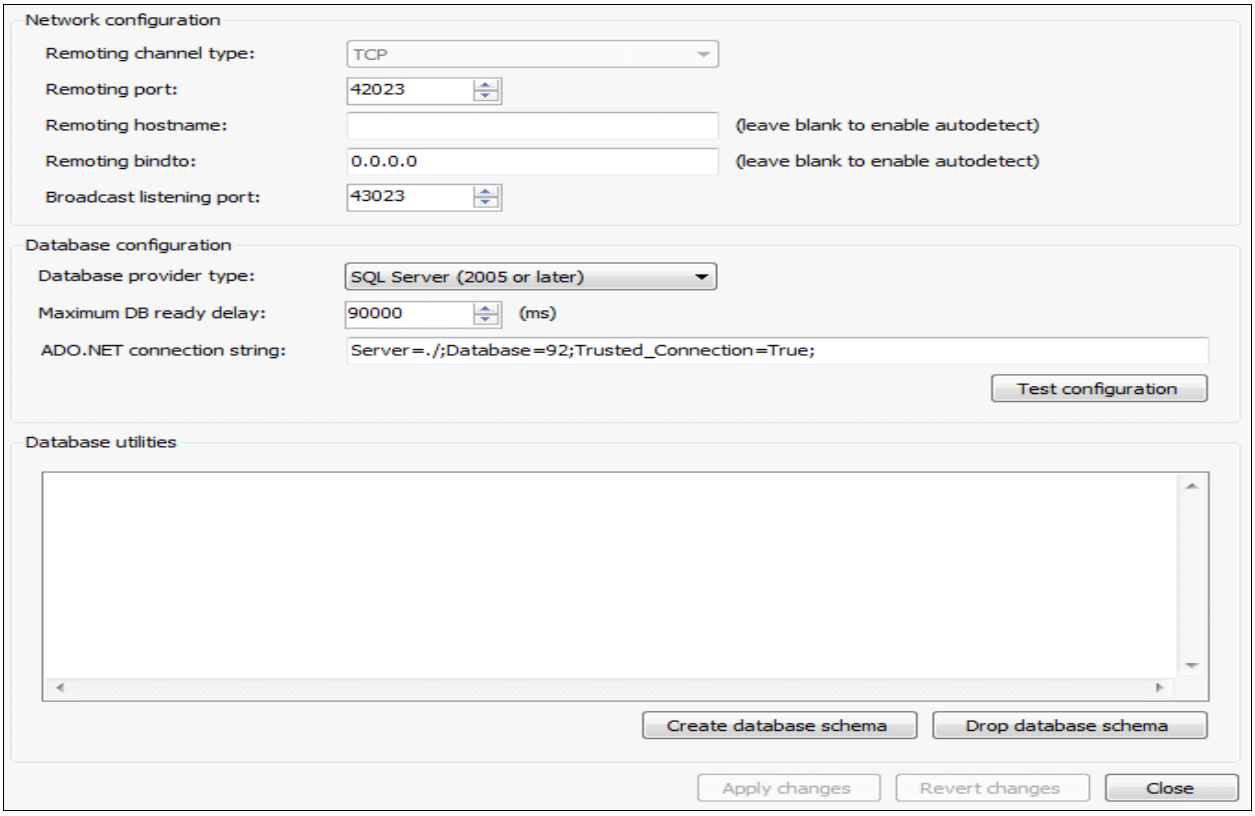
	server on the network. If there is a problem with Automatic Discovery use manually specified instead. The broadcast port must be the same as the broadcast listening port specified on the server configuration. The port values should only be changed if the default ports are being used by another application.
Port:	Specifies the server port that the MorphoManager Server is accepting client connections on. The default port is: 42100.
Remoting channel type:	Specifies whether the client/server communication should be unencrypted (TCP) or encrypted (Encrypted TCP). This setting must match the setting on the MorphoManager Server. The default is unencrypted (TCP).
Enable Automatic Login:	When enabled, the MorphoManager client will use the username and password entered here to login automatically. This can be a security problem, and should be used on clients that are secured by other means or have only one user. It is primarily used for convenience so the user does not have to enter their user name and password if it is unnecessary.

Apply the settings required and click on **Apply changes** and then **Close**.

© Refer to End User License Agreement for Copyright Notice

Advanced Server Configuration

The MorphoManager Advanced Server Configuration can be found by clicking on the start menu, then selecting “MorphoManager”, followed by “Server”, and then “Advanced Server Configuration”.



Remoting Channel Type:	Specifies whether client/server communication is to be encrypted. Default setting is unencrypted (TCP). This setting must be applied at all clients.
Remoting Port:	This is the port that the client will communicate with the server on. It must be the same as the one specified in the client configuration.
Remoting Hostname:	This is the hostname that the client will connect to. This must be the same as the hostname specified in the client configuration. This should be left blank by default.
Remoting Bindto:	If you have more than one IP address on your PC, and you want to force MorphoManager to use a specific IP, please enter it here (**Advanced users only**).
Broadcast Listening Port:	This is the port that the auto detection of servers operates on. It must be the same as the port specified in the client configuration.

© Refer to End User License Agreement for Copyright Notice

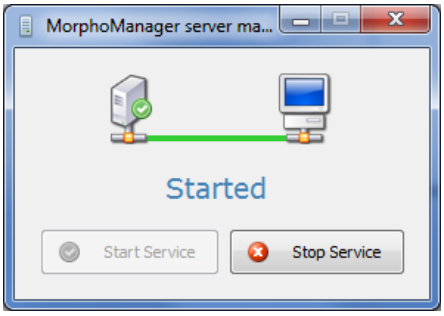
Database Provider Type:	There are two database provider types: • SQL Server (2005 or later) • SQL Server Compact Edition 4.0 SQL server Compact Edition 4.0 is selected by default and is the preferred option for smaller installations. The SQL Server 2005 or later edition is used on larger installations, or where an existing SQL Server is already available.
Maximum DB Ready Delay:	Maximum amount of time to wait for the database to be available.
ADO.Net Connection String:	This is the connection string that will be used to connect to the database. Enter the connection string and click **Test Connection**. Ensure the connection is successful before applying changes.
Drop Database Schema:	Dropping a database schema will remove all tables and all data from the database. This is a non-recoverable operation and cannot be undone. Revert changes will not undo this operation. A prompt will be displayed confirming this action.
Create Database Schema:	Creating a database schema should only be performed on a new empty database or an existing database that has had a drop schema operation performed on it. This operation will set up a database and create all the tables and default data for MorphoManager.
Apply Changes:	When all the settings are correct click **Apply Changes** to save the changes.
Revert Changes:	Reverts all changes back to their last saved state. **A drop database schema cannot be reverted**.

© Refer to End User License Agreement for Copyright Notice

Server Manager

The MorphoManager Server Manager can be found by clicking on the start menu, then selecting “MorphoManager”, followed by “Server” and then “Server Manager”.

The server manager is used to start and stop the MorphoManager server. Stopping the server will stop all clients from operating. This should only be performed if instructed by the support staff.

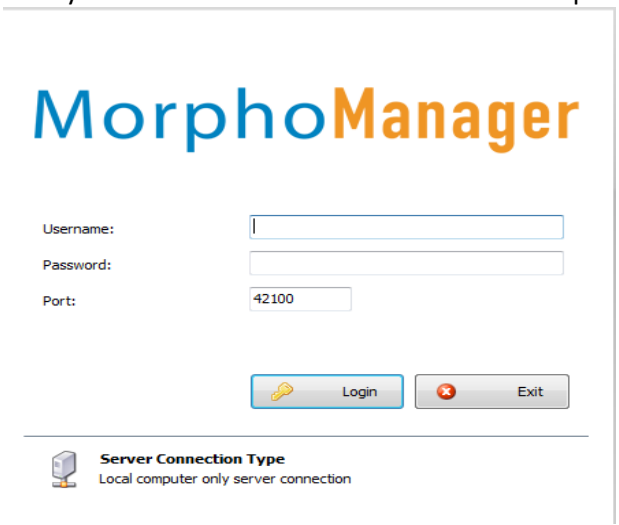


Running MorphoManager Login

MorphoManager Client software requires a username and password to be entered before starting.

By default the username is **administrator** and the Password is **password**.

Once you have entered the correct username & password, click **Login** to login.

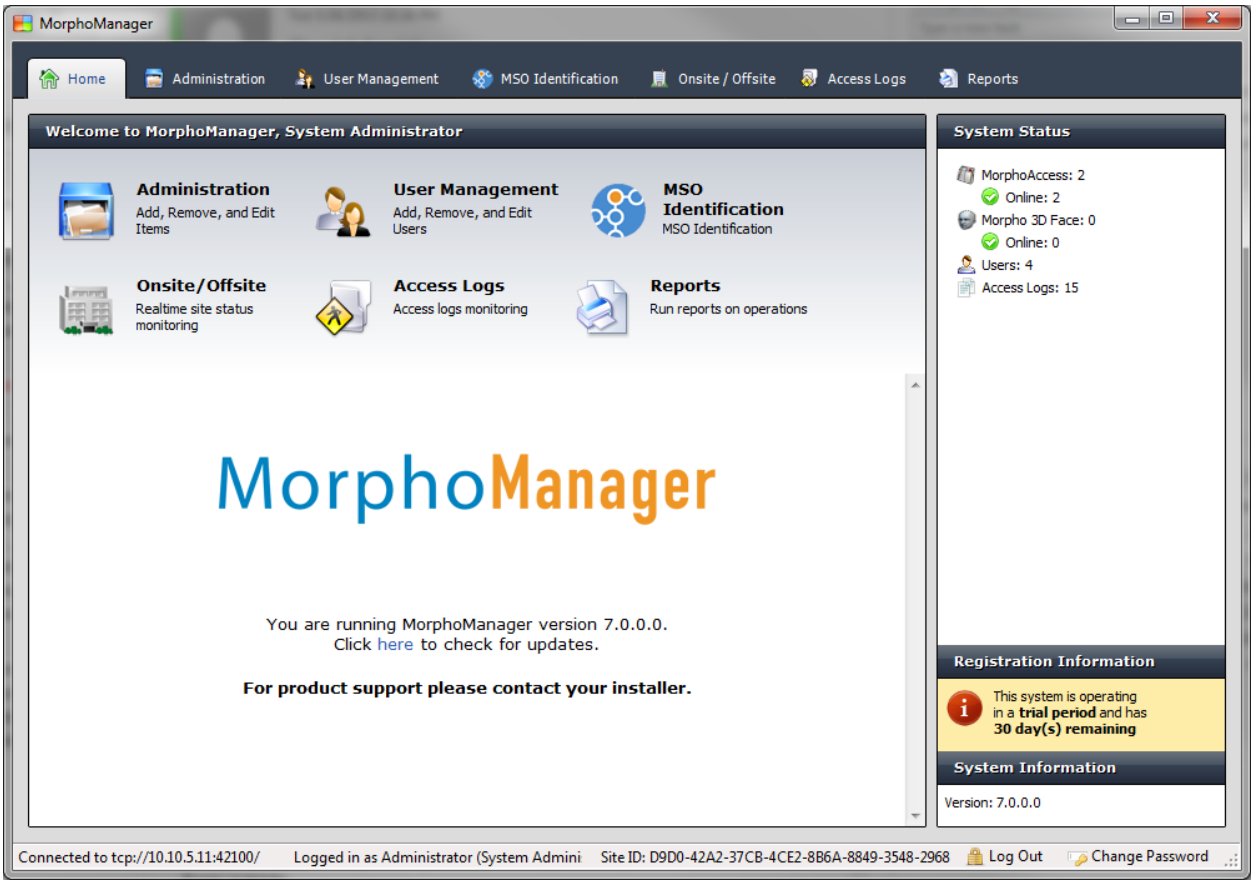


© Refer to End User License Agreement for Copyright Notice

Home Screen

At the top of the home screen, there is a set of tabs (**Home, Administration, User Management, MSO Identification, Onsite/Offsite, Access Logs, and Reports**) and a set of buttons on the home screen. Select an item to enter that section.

At the bottom of the home screen is a link to MorphoManager updates. If you have access to the internet, you will be directed to this area which will be updated with news and information regarding MorphoManager patches and important messages.



The right hand side of the screen displays the system status and system information. System status contains a count of the total number of Biometric Devices and their current status. It also contains a count of the total number of users within the system and the total number of access logs. System Information contains the installed version number, and your server serial code.

© Refer to End User License Agreement for Copyright Notice

Administration

The administration section is used to configure and setup MorphoManager. Error and event logs are also viewable in this section.

When creating or editing an item, a coloured text entry box means the information is required and must be filled in before the item can be finished and saved.

Operators

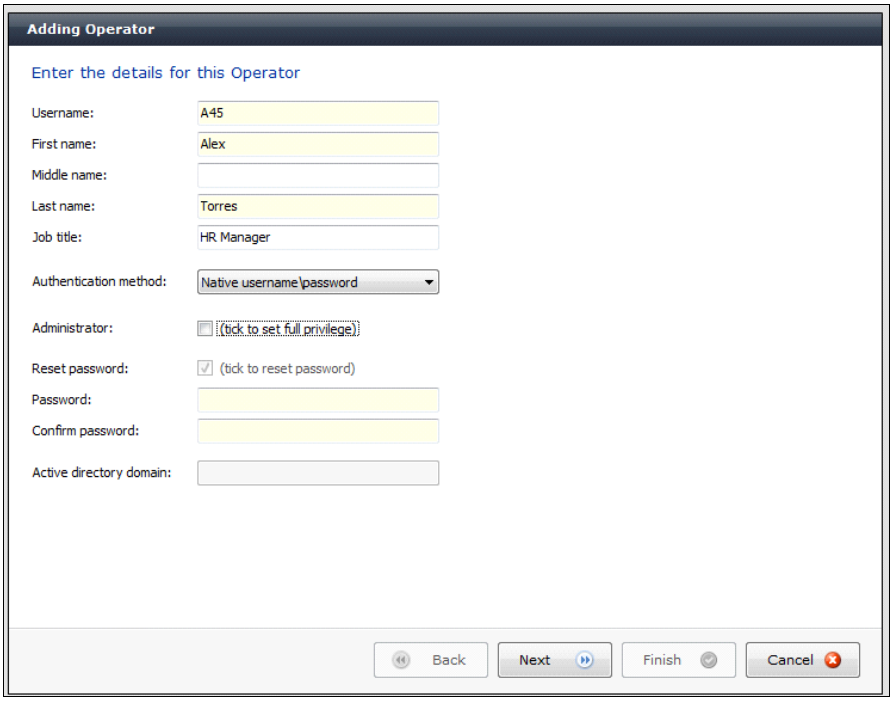
An operator is a person who uses the MorphoManager Client software. Operators are the only people who can login to the MorphoManager application. The Administrator operator has full access to all functions. Other operators with limited rights can be created.

In the panel to the right, you will see that a default Operator has been created as the System Administrator. This operator cannot be deleted or modified. This operator has access to every part of Bio Manager and so keeping the password for this user secure is essential.

Creating a new Operator

Select the **Operator** section on the left and click **Add**

Screen 1 – Operator Details

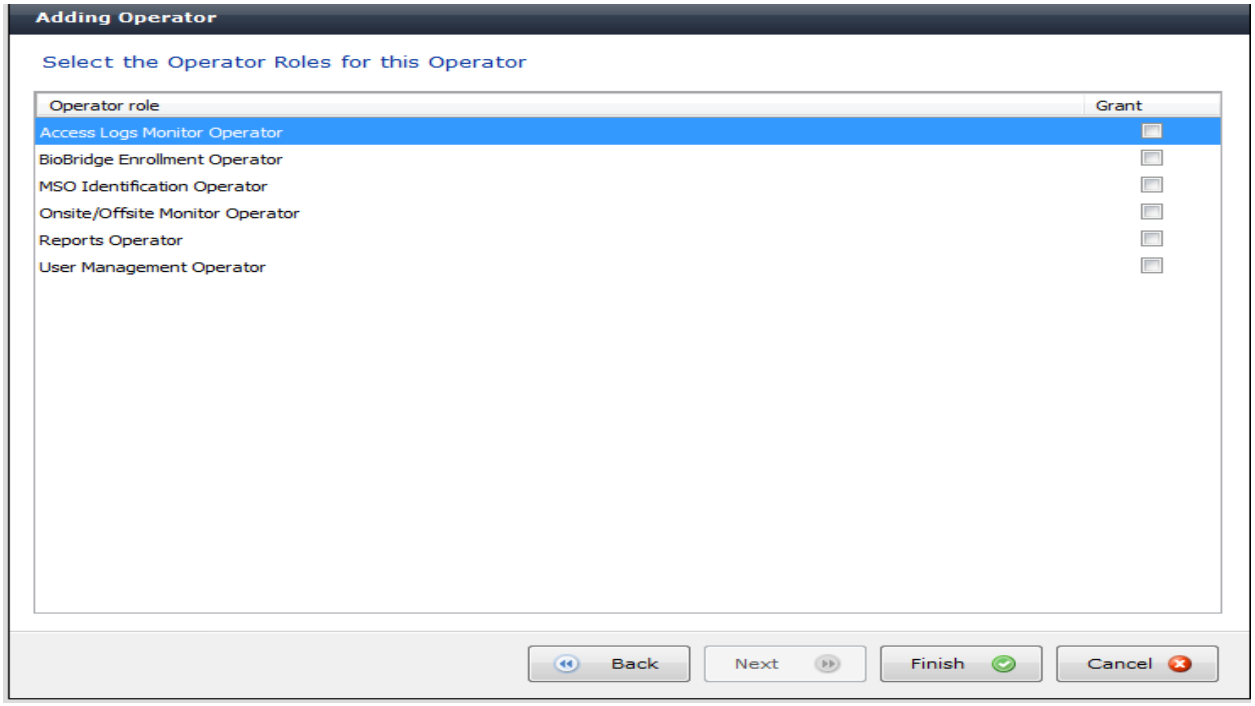


© Refer to End User License Agreement for Copyright Notice

Username:	This will be entered at the login screen (must be greater than 4 characters).
First / Middle / Last Name:	The first, middle and last name of the operator being added (First and Last names are mandatory fields).
Job Title:	The job function that this operator performs.
Authentication Method:	There are two methods for password authentication.
Native Username / Password:	This method uses the username and password entered in this screen.
Active Directory Integration:	This method uses the Windows Active directory to authenticate passwords. The username must match an existing user in the active directory. The active directory domain must be specified to use this option.
Administrator:	Select this option to provide full administrator rights to this user (not recommended).

Screen 2 – Operator Roles

Select the Operator Roles this operator will be allowed to perform. More than one Operator Role can be selected and the Operator will have access to all of the functions that the roles allow.



© Refer to End User License Agreement for Copyright Notice

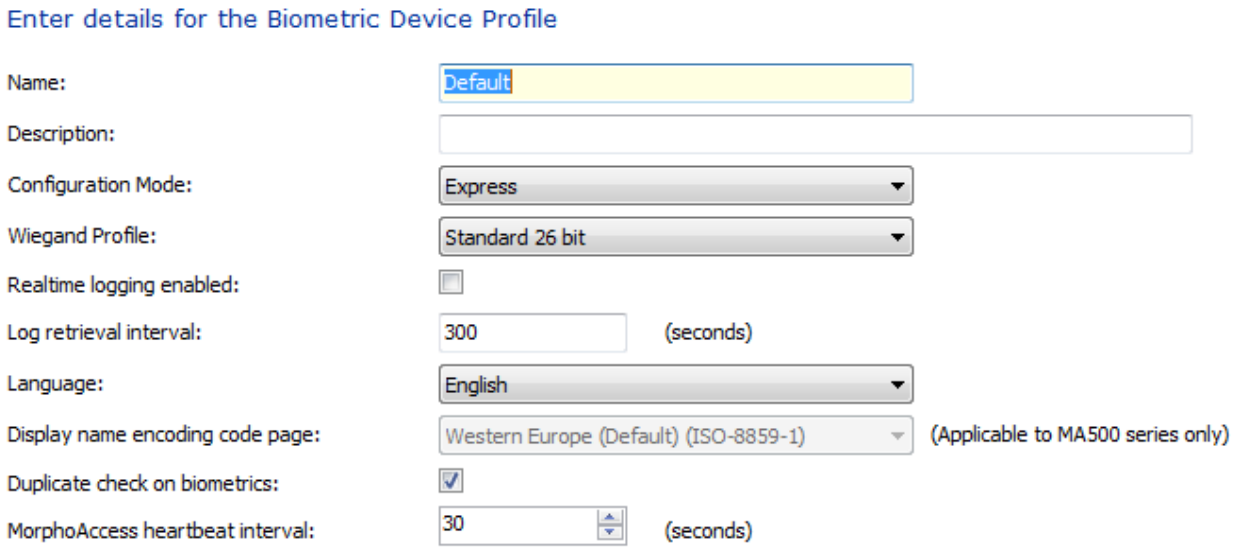
Biometric Device Profile

The Biometric Device Profile will define common settings and parameters for one or more biometric devices. This profile can be applied when adding units into the system from the Biometric Device section of Administration.

Creating a new Biometric Device Profile (Express)

Select the **Biometric Device Profile** section of Administration and click **Add.**

Screen 1 – Configuration Details



Name: Name the profile anything up to fifty characters.

Description: Give the profile a description of up to one hundred characters.

Configuration Mode: Can be either Express, Advanced, or External, but in this example select **Express**.

Wiegand Profile: Select the Wiegand Profile to be utilized on the Biometric Device.

If you are utilizing the Wiegand output on the Biometric Devices, you will need to set the Wiegand Profile for the Biometric Device(s) here. The Wiegand Profile you choose for your devices should match the one being utilized for your users which is set in the User Group section of this manual.

Realtime Logging Enabled: Enable this tick box to retrieve the access logs in real time. MorphoManager will automatically retrieve the new logs instantly for every finger presentation. By default, this setting will be disabled. It can be enabled only after configuring the settings in System Configuration.

© Refer to End User License Agreement for Copyright Notice

Log Retrieval Interval: Each Biometric Device is periodically polled to collect any new data and remove stored data from memory. This is the amount of time between each polling sequence. The default is 300 seconds.

Language: Choose the language you wish to use on your Biometric Device display screen.

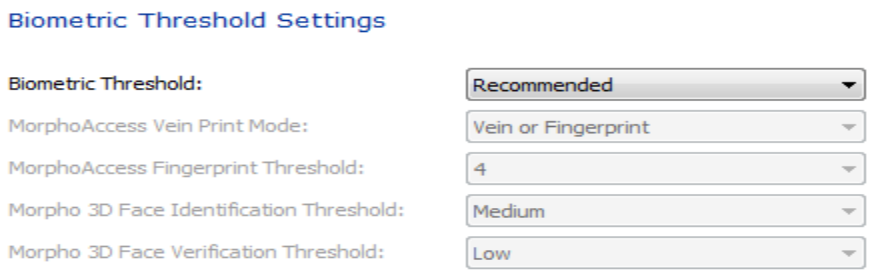
Display Name Endoding Code Page: This section allows you to set encoding for the display name for downloading to MA2G devices. Your choices will be:

- Western Europe (Default) (ISO-8859-1)
- Central Europe (ISO-8859-2)
- Southern Europe (ISO-8859-3)
- Baltic (ISO-8859-4)
- Cyrillic (ISO-8859-5)
- Arabic (ISO-8859-6)
- Greek (ISO-8859-7)
- Hebrew (ISO-8859-8)
- Turkish (ISO-8859-9)
- Latin 9 (ISO-8859-15)

Duplicate Check on Biometrics: When turned on this will check users when being enrolled for duplicate fingerprints in the system.

Morpho Access Heartbeat Interval: This will determine how often the system checks to see if the Biometric Devices are online.

Screen 2 – Biometric Threshold Settings



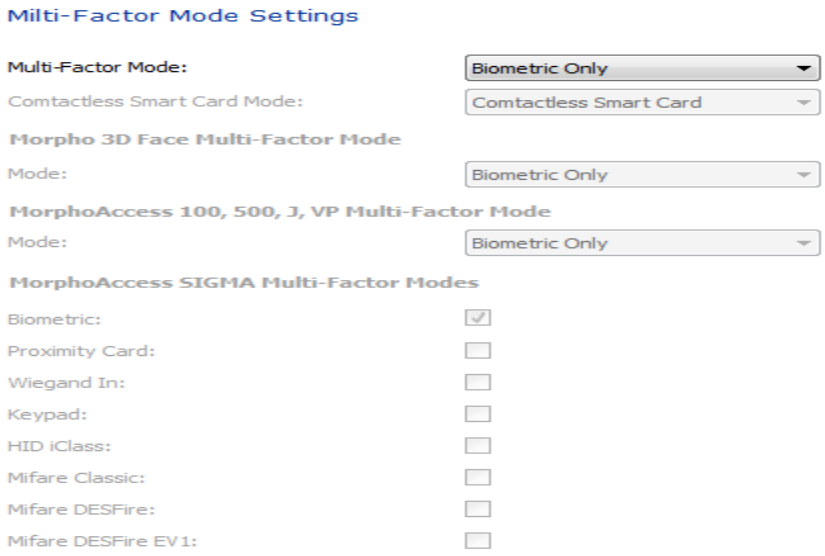
These values determines the cut off point for a biometric presentation to match with a stored template. A higher value will lead to more false rejections for people with lower quality fingerprints. Lowering the value allows people with lower quality fingerprints to be authenticated, but if the value is too low there

© Refer to End User License Agreement for Copyright Notice

is a possibility of a false acceptance. This is only enabled when the Biometric Device type has been detected.

Biometric Threshold: The default is Recommended. However, it can be set to Low, High, Very High, and Custom. Choosing the Custom setting will allow you to set individual threshold properties for the four device types greyed out in the screenshot above.

Screen 3 - Multi-Factor Mode Settings



This area dictates the matching mode used by the Biometric Devices. This is only enabled when the Biometric Device type has been detected.

Multi-Factor Mode: There are seven individual options and the ability to do a custom selection for each hardware family. The options are as follows:

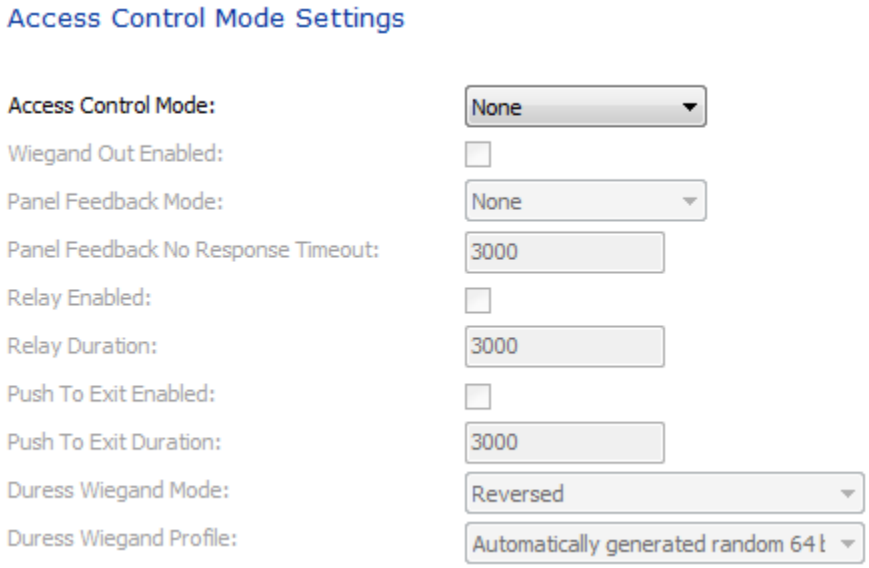
- **Biometric Only** – Select this option if the Biometric Device is used for identification by biometrics only. With this option, a person does not have to provide any input other than the biometric utilized by that device for identification.
- **Wiegand In** – This option authenticates Wiegand Input to match against a biometric template.
- **Keypad –** This option allows the user to enter a user code or a pin number via the terminal keypad to match against a biometric template.
- **Proximity Card –** This option allows Proximity Cards to be utilized with a Proximity card capable device. Fingerprints will be stored on the device instead of card.
- **HID iClass–** This option allows HID iClass Cards to be utilized with an HID iClass card capable device.

© Refer to End User License Agreement for Copyright Notice

- **Mifare Classic –** This option allows Mifare Classic Cards to be utilized on a Mifare Classic capable device
- **Mifare DESFire -** This option allows Mifare DESFire Cards to be utilized on a Mifare DESFire capable device
- **Custom -** The Custom setting will allow you to set individual properties for each of the three hardware families (The Morpho 3D Face, MorphoAccess 100, 500, J, and VP, and MorphoAccess Sigma) which are greyed out in the screenshot above.

It is always recommended to use Biometric Only mode. However, depending on how the MorphoAccess will be used any of the above options can be selected.

Screen 4 – Access Control Mode Setttings



This area sets the properties for Access Control on your Biometric Devices.

Access Control Mode: There are four modes available, None, Integrated, Stand-alone, and Custom. The default here is None. Which disables all other items. In Integrated you can set the Panel Feedback Mode and Panel Feedback No Response Timeout properties. In Stand-alone mode you can set the properties on Relay Enabled, Relay Duration, Push to Exit Enabled, and Push to Exit Duration. And, lastly in Custom mode you can set all properties.

Wiegand Out Enabled: This will determine whether or not your biometric device will output a Wiegand value.

Panel Feedback Mode: Allows you to choose between LEDIN and RS485.

© Refer to End User License Agreement for Copyright Notice

Panel Feedback No Response Timeout: This value will determine the length of response time allowed from the Access Control Panel.

Relay Enabled: Each Biometric Device has an on board relay that can be used to control an external device on successful presentation of a fingerprint. Use this option to activate the relay when a user is authenticated.

Relay Duration: If the relay is activated, this value will determine the length of activation time.

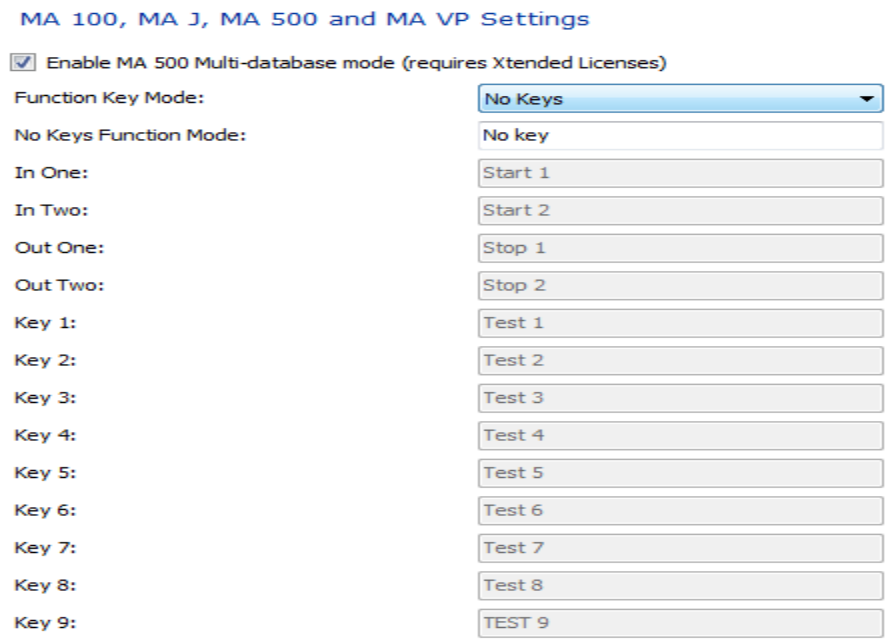
Push To Exit Enabled: This allows the Access Panel to open a door even though the user is not identified on device.

Push to Exit Duration: This sets the length of time the door will remain open if Push to Exit is enabled.

Duress Wiegand Mode: This determines whether the use of Wiegand for duress finger is Disabled, Reversed, or Custom.

Durress Wiegand Profile: If the Durress Wiegand Mode is Custom, this will set the Wiegand Profile to be used during presentation of a duress finger.

Screen 5 – Function Key Mode for MA 100, J, 500, and VP Family

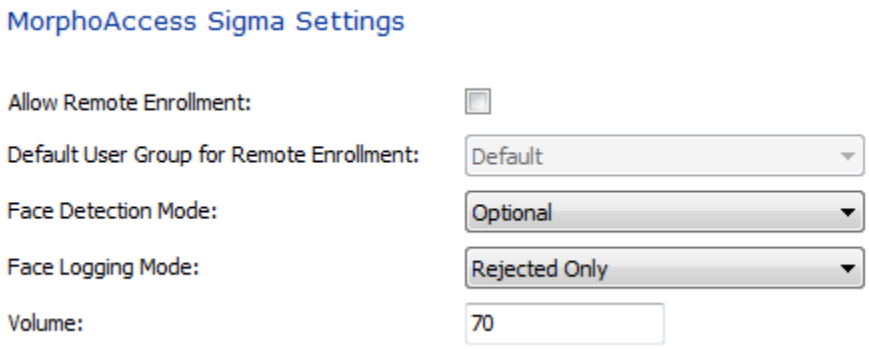


Enable MA 500 Multi-database Mode: This will allow you to enable the Multi-database mode on this family of devices if they have the proper license installed.

© Refer to End User License Agreement for Copyright Notice

Function Key Mode: This area determines what function keys, if any, will be available on a device (where applicable). Options in this drop down are No Keys,Two Keys, Four Keys, or Nine Keys to be displayed on device. Each key enabled in the list of keys can be renamed to meet individual needs for events in Time & Attendance and Access Log records.

Screen 6 – MorphoAccess SIGMA Settings



Allow Remote Enrollment: Allows users to be enrolled on selected MorphoAccess Sigmas. Once a user is enrolled on a device, the software will retrieve the user from the device, be inserted into the MorphoManager database, and then distributed to any other Sigmas as per User Policy settings.

Default User Group For Remote Enrollment: Remotely enrolled users will be placed in the User Policy selected.

Face Detection Mode: Allows you to set the Sigma units to capture a photo when someone is presenting to the device (this works in conjunction with the Face Logging Mode). There are four individual options :

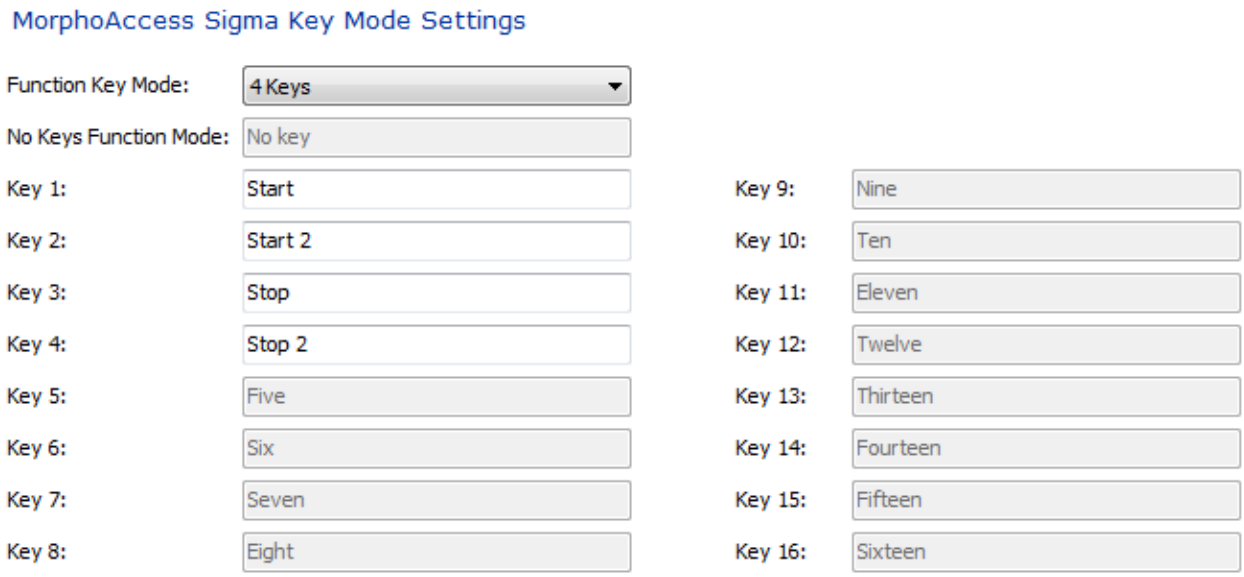
- **Disabled** – Use this option if you want to completely turn off Face Detection photo capture.
- **None –** Will take a 1 photo for the log whether or not a face is detected.
- **Optional –** Takes a series of pictures and choses the best face it detects out of them for the log. However, if the user is rejected (biometric mismatch) AND it doesn't detect a face, no photo will be used.
- **Mandatory –** Takes a picture in all scenarios (rejected or accepted presentation).

Face Logging Mode: This determines whether or not Rejected, Accepted, or Rejected and Accepted presentations to the Sigma are logged. This works in conjunction with Face Detection Mode.

Volume: Set the device volume level to anything from 0-100.

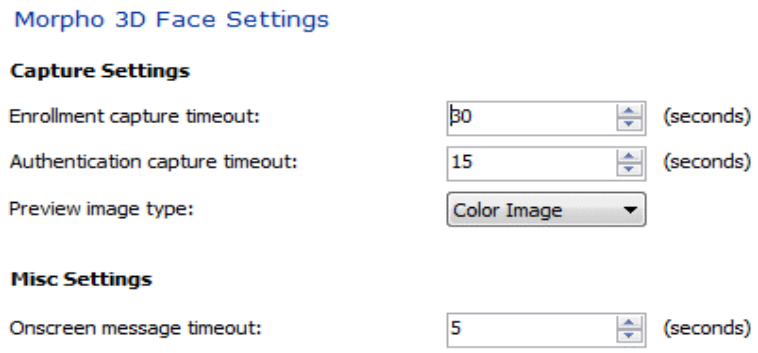
© Refer to End User License Agreement for Copyright Notice

Screen 7 – MorphoAccess Sigma Key Mode Settings



Function Key Mode: This area determines what function keys, if any, will be available on a MA Sigma. Options in this drop down are No Keys, Four Keys, or Sixteen Keys to be displayed on device. Each key enabled in the list of keys can be renamed to meet individual needs for events in Time & Attendance and Access Log records. In Sixteen Keys mode any key name field left blank will not show as a button on the device screen.

Screen 8 – Morpho 3D Face Settings



Enrollment Capture Timeout: Time the device will attempt to capture a 3D Face during enrollment (default 30 seconds).

Authentication Capture Timeout: The maximum time the device will attempt to authenticate/verify a user in verification mode.

Preview Image Type: Specifies whether to show the enrollment preview image in color or 3D face surface mode.

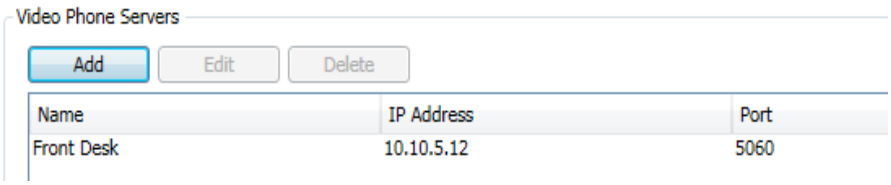
© Refer to End User License Agreement for Copyright Notice

Onscreen Message Timeout: The amount of time that an on screen messages will be shown to the user.

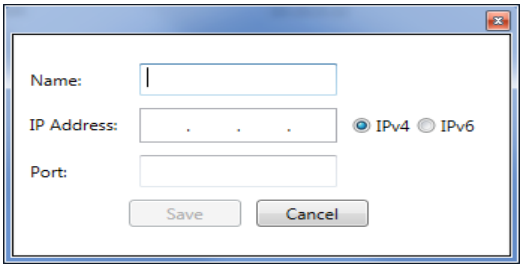
Screen 9 – Video Phone Server Settings

To utilize the Video Phone features of the Sigma you will need to add your server here. Adding a Video Phone Server is not mandatory for creating a Biometric Device Profile and you can click **Finish** on this screen with or without adding the Video Phone Server.

Video Phone Server Settings



Click **Add** to add the Name, IP Address and Port of your Video Phone Server. Click **Save** when finished.

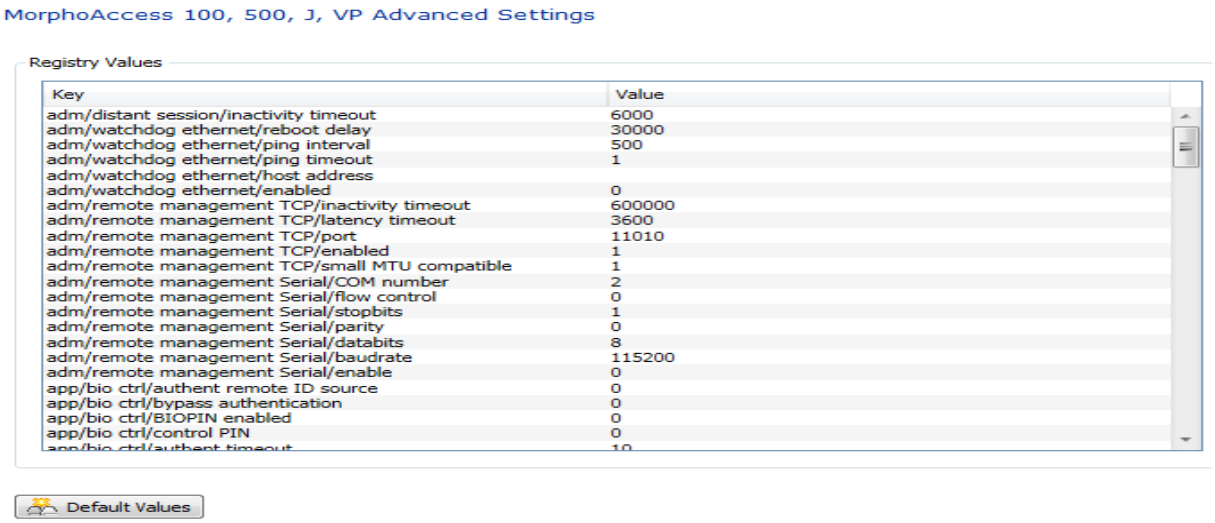


© Refer to End User License Agreement for Copyright Notice

Creating a new Biometric Device Profile (Advanced)

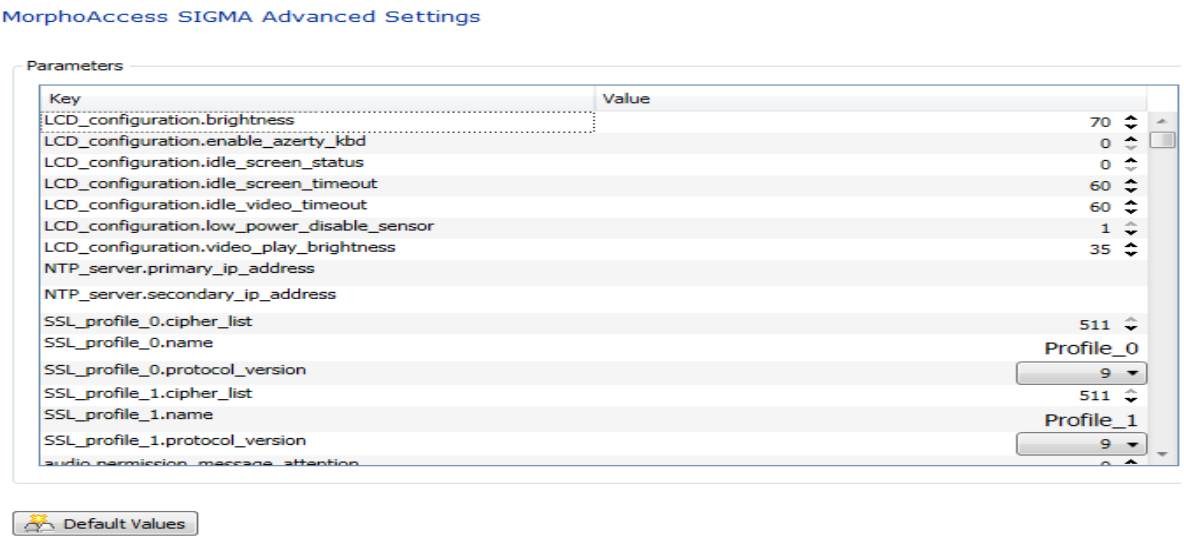
Select the **Biometric Device Profile** section of Administration and click **Add.** This time on Screen 1 you will select **Advanced** from the Configuration Mode drop down. The Advanced profile Screen 2 allows you to configure the various parameters for the Morpho Access 100, 500, J, and VP.

Screen 2- Advanced Parameters for MorphoAccess 100, 500, J, and VP



If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

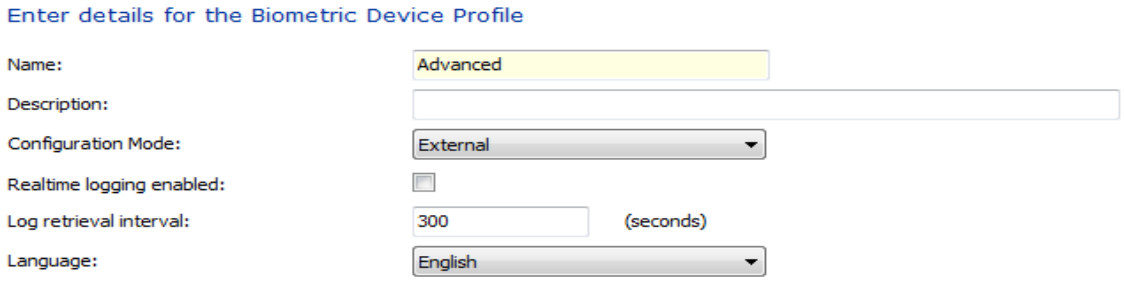
Screen 3 – Advanced Parameters for MorphoAccess SIGMA



Information for the wizard screens that follow Screen 3 above can be found in the section for **Creating a new Biometric Device Profile (Express).**

© Refer to End User License Agreement for Copyright Notice

Creating a new Biometric Device Profile (External)



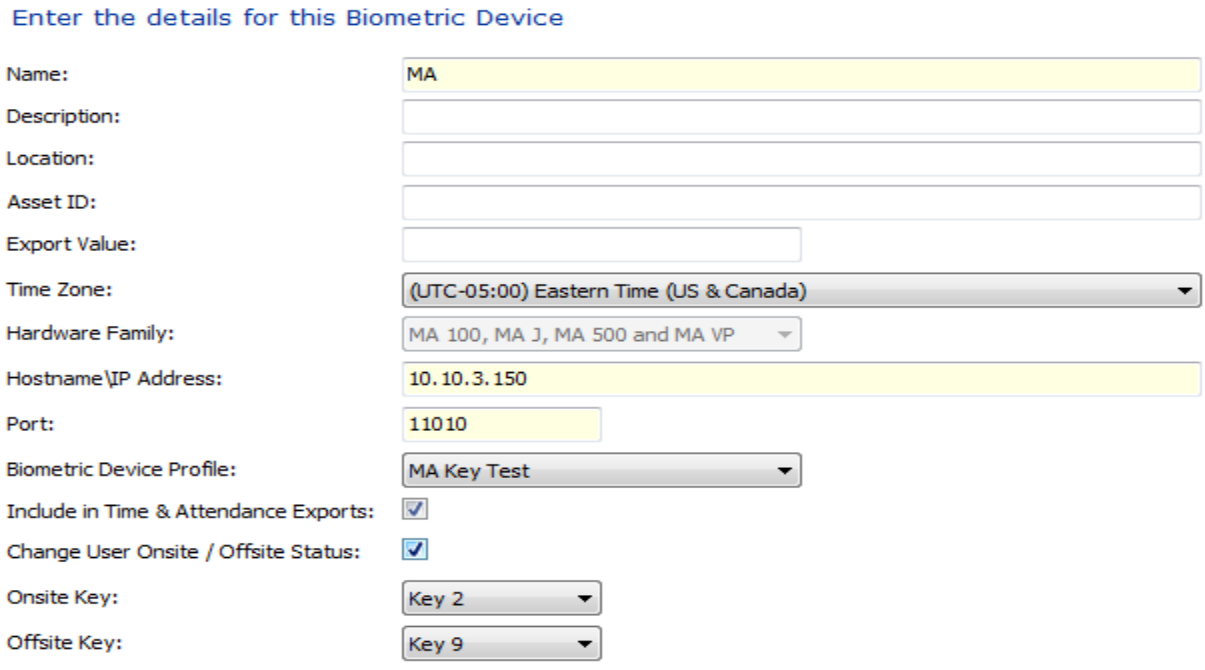
Selecting External for your Configuration Mode allows you to set all parameters on device or via external software that interfaces with the Biometric Device parameters. When selecting External mode this will be the only wizard screen you will utilize.

Biometric Device

Biometic devices from three different hardware families can be added here; the MA 100, MA J, MA 500, and MA VP family, the MA Sigma family, and the Morpho 3D Face.

Create a Biometric Device

Select the **Biometic Device** section of Administration and then click **Add** in the toolbar.



Name: The name of the Biometric Device.

Description: A description of the Biometric Device.

Location: The installed location of the Biometric Device.

© Refer to End User License Agreement for Copyright Notice

Export Value: This value is typically used for Access log exporting when the MorphoManager data needs to be exported to a third-party payroll package. It can have a maximum of 20 characters.
When the access logs are exported, the value specified here will be used as the Biometric Device name in the output exported file. This again depends on the particular requirements of the payroll package and the access log exporter that is configured in the System configuration under T&A General settings.

Time Zone: It is important that this field is entered correctly as it will affect the time displayed on the Biometric Device and in which time zone access logs are recorded.

Hardware Family: Corresponds to the model of the Biometric. As mentioned above Biometic Devices from three different hardware families can be added here; the MA 100, MA J, MA 500, and MA VP family, the MA Sigma family, and the Morpho 3D Face.

Hostname \ IP address: This value is critical. Enter the IP address of the selected Biometric Device..

The IP Address on each device must be manually assigned and must be within the IP range of the network. The IP address must not be used by any other device on the network.

Port: This is the default that MorphoManager software is expecting.

Biometric Device Profile: This will allow a common settings and parameters profile to be set for the device added. The profile itself is created in the Biometric Device Profile section of Administration.

Include in Time & Attendance Exports: Enable if the gathered data is to be sent to a Payroll or Rostering package.

Change User Onsite/Offsite Status: Enable if Onsite/Offsite events are to be recorded.

Onsite Key: Determines which function key on the device will be utilized to set a user Onsite.

Offsite Key: Determines which function key on the device will be utilized to set a user Offsite.

After all information has been entered click **Finish** to save the changes or **Cancel** to discard the changes. You will now see the new Biometric Device in the window and its status will be Online, provided the PC

© Refer to End User License Agreement for Copyright Notice

and device are correctly connected and configured. The Tasks column shows the count of the queued or the failed tasks.

Modify a Biometric Device

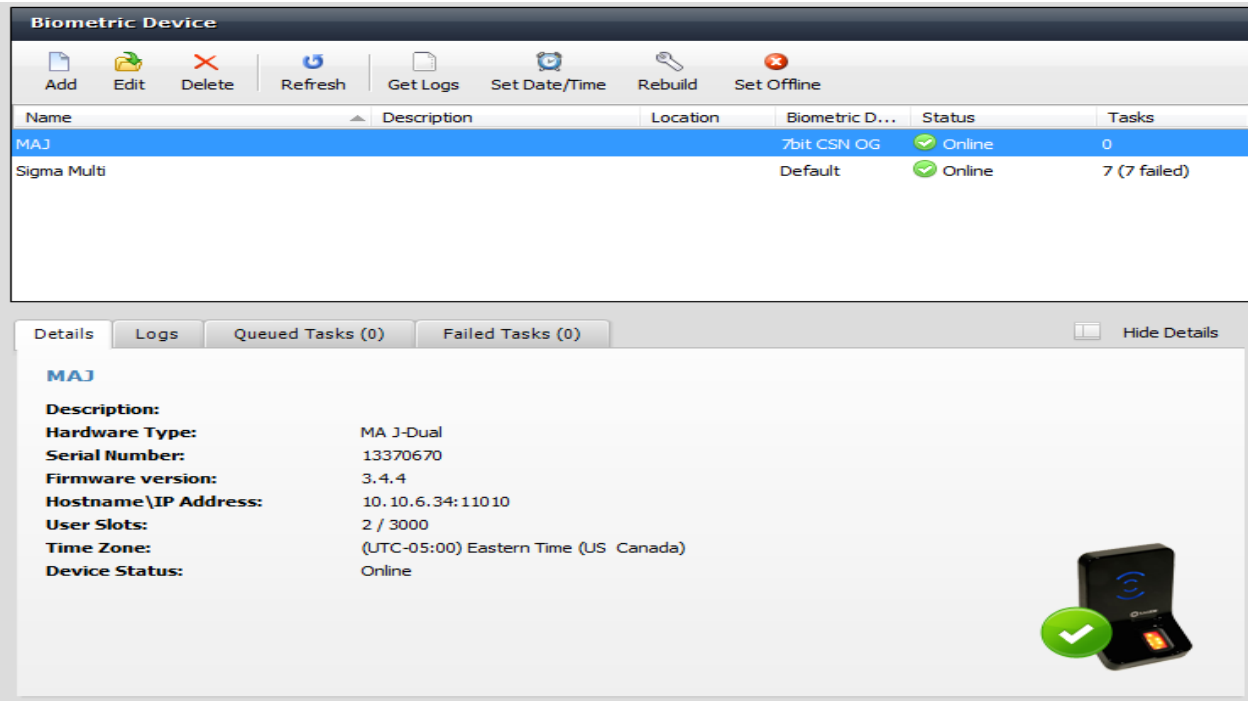
To modify a Biometric Device, left click on a device and click **Edit** on the toolbar. A wizard will open showing the information entered when the Biometric Device was created. Change any of the values required and click **Finish** to save changes or **Cancel** to discard changes.

Delete a Biometric Device

Select the device to delete and click **Delete** on the toolbar. To delete a Biometric Device, you must remove ALL user policy and user access. A Biometric Device cannot be deleted if any user still has access. This ensures that all user access has been correctly revoked.

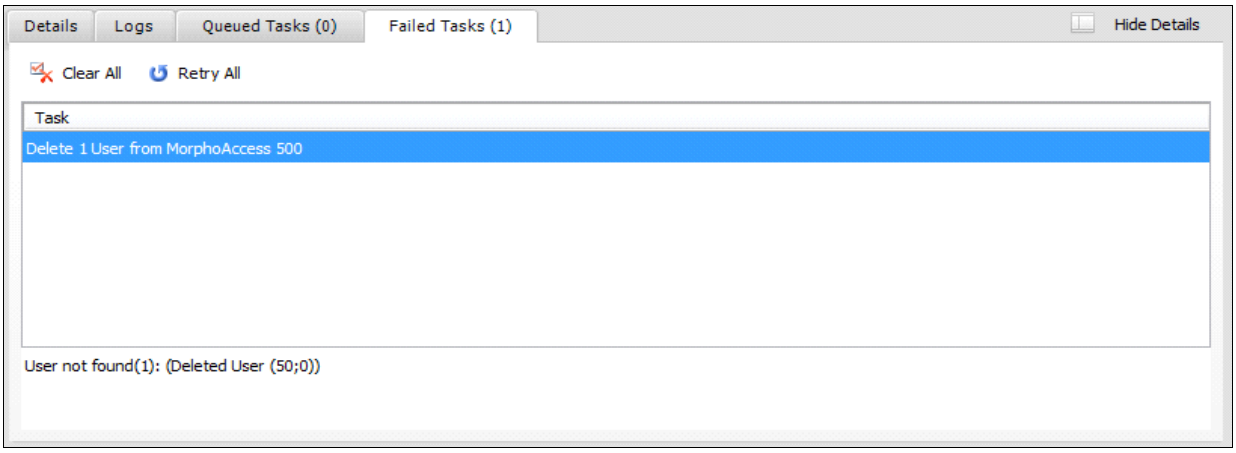
Biometric Device Status and Tasks

When viewing a list of Biometric Device, the status column indicates the current status of each Biometric Device. Online means the Biometric Device is responding to communication requests. Offline means that the Biometric Device is not responding to communication requests. The tasks column indicates the number of tasks remaining for the Biometric Device to process. Clicking on the **Queued Tasks** and **Failed Tasks** tab in the details section allows these tasks to be reviewed. Clicking on **Logs** allows review of access logs retrieved from that Biometric Device.



© Refer to End User License Agreement for Copyright Notice

Troubleshooting and Maintenance



In the example screen above, the “Delete User” task failed. The message below explains the reason for the failed task.

Toolbar Functionality

Get Logs – Will download the currently stored transactions from the Biometric Device into MorphoManager. Inbuilt into MorphoManager is an automatic retrieval that, by default, occurs every 5 minutes.

Set Date/Time – Updates the Biometric Device’s clock to the time on the server.
This command is run automatically once a day at the time specified in the system configuration.

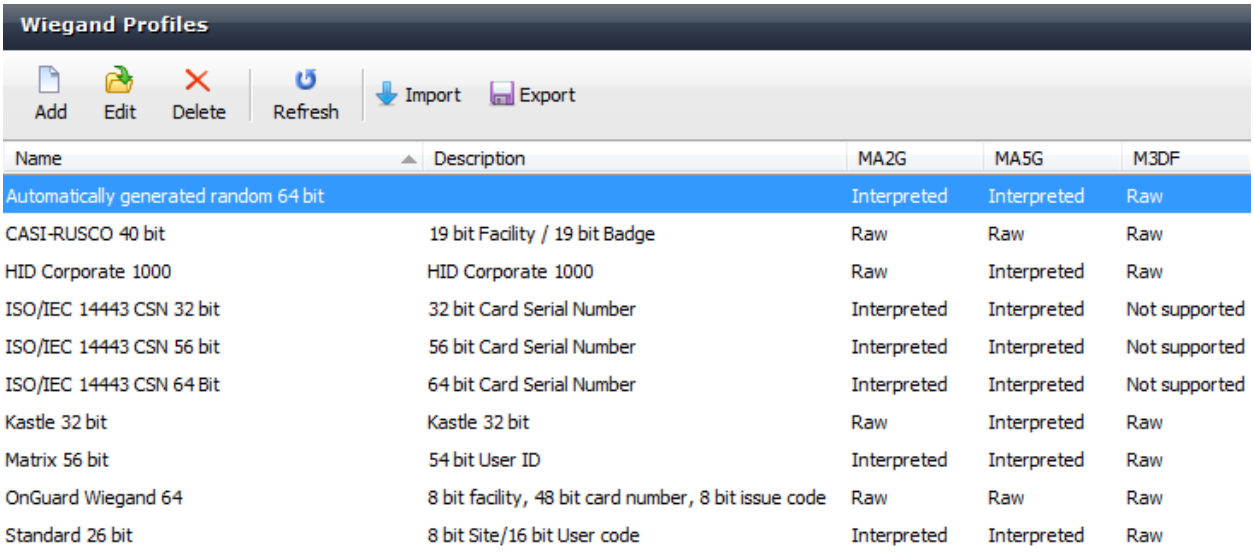
Rebuild – The rebuild function will remove all users from a Biometric Device and upload the users who are permitted access. This function should only be used if the device is not operating as expected. Unexpected behavior could occur if a device was moved from another site and contained existing users from that site. During normal operation any users who are added or deleted through user management are updated on the Biometric Device in real time.

Set Online – MorphoManager monitors and displays the status of every Biometric Device. If a device has gone offline, clicking **Set Online** will attempt to connect to the device and go online. The status of the Biometric Device will change to “Pending Online” while the connection is occurring. If there is a problem connecting to the Biometric Device the status will revert to “Offline”.

© Refer to End User License Agreement for Copyright Notice

Wiegand Profiles

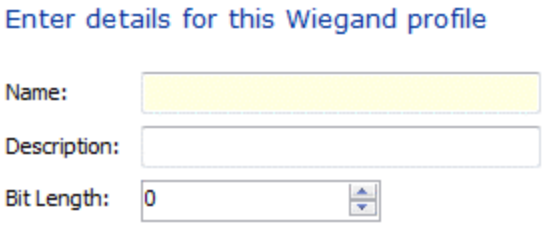
This section allows you to view, add, edit & delete Wiegand Profiles in MorphoManager. Wiegand Profiles define what information is output over the Wiegand Out interface of the Morpho Biometric Devices when a user is identified. This is most typically used in conjunction with an Access Control System.



Name	Description	MA2G	MA5G	M3DF
Automatically generated random 64 bit		Interpreted	Interpreted	Raw
CASI-RUSCO 40 bit	19 bit Facility / 19 bit Badge	Raw	Raw	Raw
HID Corporate 1000	HID Corporate 1000	Raw	Interpreted	Raw
ISO/IEC 14443 CSN 32 bit	32 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 56 bit	56 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 64 Bit	64 bit Card Serial Number	Interpreted	Interpreted	Not supported
Kastle 32 bit	Kastle 32 bit	Raw	Interpreted	Raw
Matrix 56 bit	54 bit User ID	Interpreted	Interpreted	Raw
OnGuard Wiegand 64	8 bit facility, 48 bit card number, 8 bit issue code	Raw	Raw	Raw
Standard 26 bit	8 bit Site/16 bit User code	Interpreted	Interpreted	Raw

Create a Wiegand Profile

Screen 1 – Configuration Details



Name: Name the profile anything up to fifty characters.

Description: Give the profile a description of up to one hundred characters.

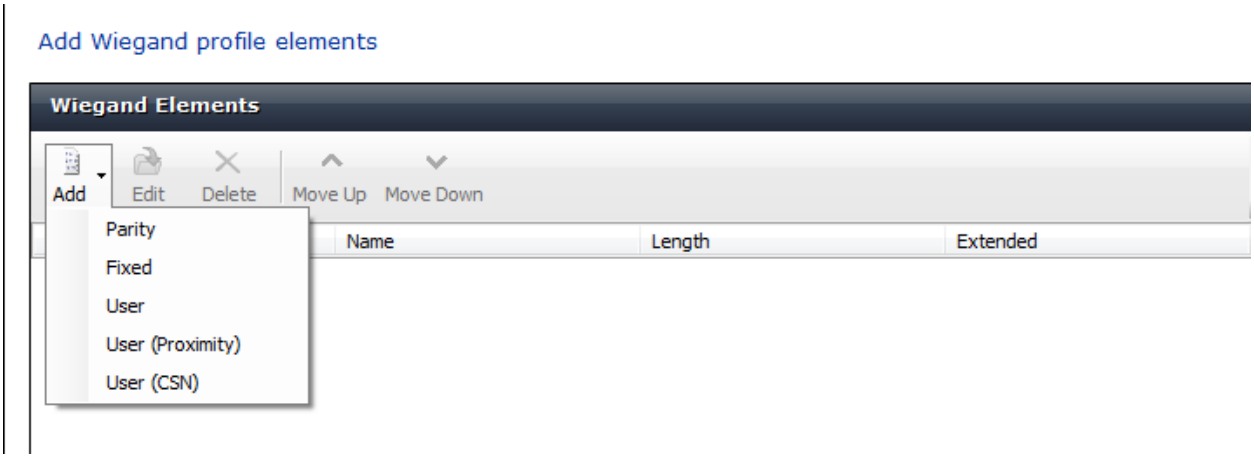
Bit Length: Designate the overall bit length needed for your profile.

Screen 2 – Wiegand Profile Elements

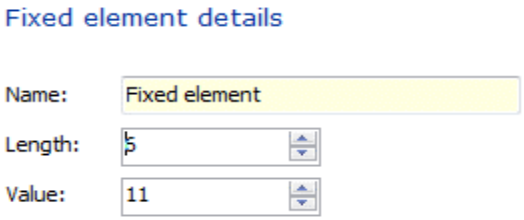
On Screen 2 you will be able to add the elements needed to make up your Wiegand Profile. Click **Add** to select the element needed from the drop down. There are five element types that can be used to construct a Wiegand Profile:

© Refer to End User License Agreement for Copyright Notice

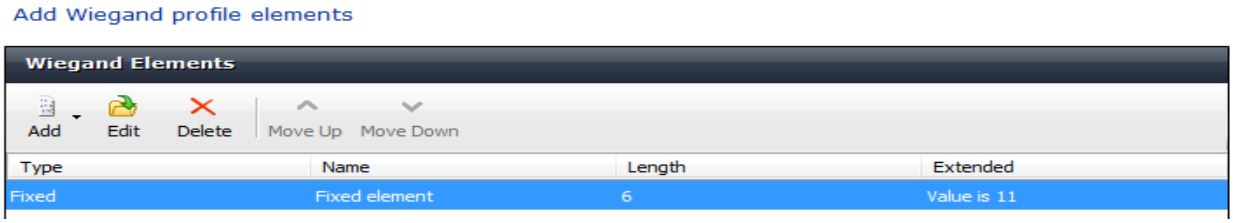
- **Parity:** Indicates a single bit that is typically used for error detection. Parity is calculated over one or more bits within the entire profile and can be Even or Odd.
- **Fixed:** Indicates a value that is common to all users of this Wiegand Profile. Typical examples of fixed values are Facility/Site codes. This value is set once in the Wiegand Profile and will then be used by all users of this Wiegand Profile.
- **User:** A value that can be entered during enrollment for each user. A typical example of a User value is a User ID.
- **User (Proximity):** Similar to the User value, this value is defined during enrollment, but is read from a connected proximity card.
- **User (CSN):** Similar to the User value, this value is defined during enrollment, but is read from an ISO/IEC 14443 smart card's serial number.



Once the element has been selected the details screen for that element can be populated as in the example below. Once the screen is populated click **Next**.



You will be take back to the Wiegand Profile element screen (below) and it will now be populated with the element you just added.



Once you have built out all of the elements needed to make up your Wiegand Profile, you can click **FINISH**.

© Refer to End User License Agreement for Copyright Notice

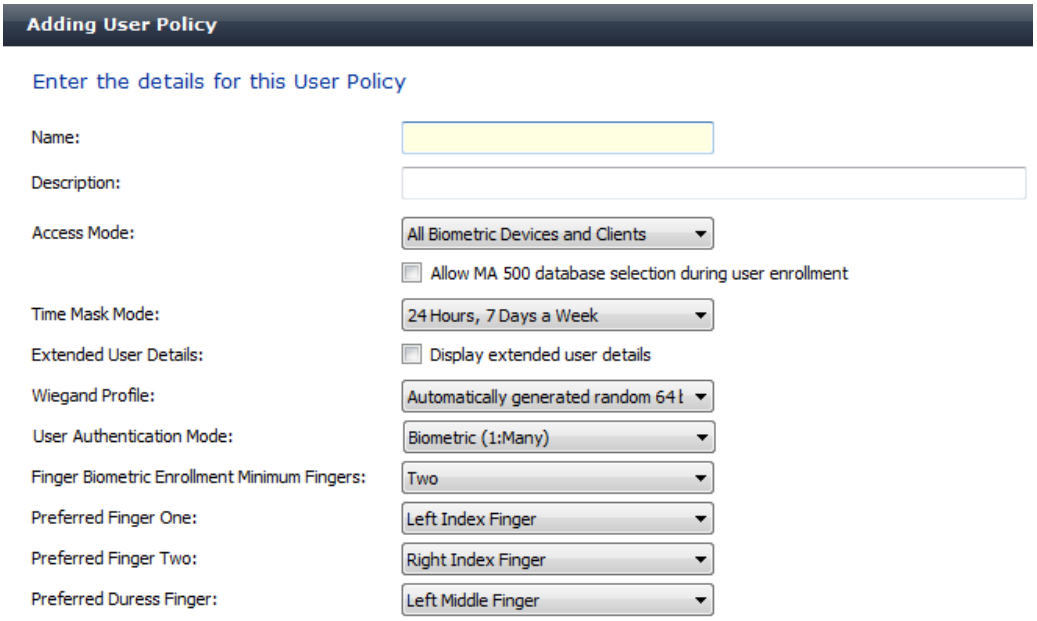
User Policy

User polices are used to apply access rights and rules to all members of the group.

Users cannot exist in the database without being assigned to a User Policy. However, a User Policy can exist without having access to any Biometric Device. This can be useful for segregating users who, for security or other reasons, should not be stored on a device.

Create a new User Policy

Screen 1 – Details



Name: Name of the user policy.

Description: Description of the purpose of the user policy.

Access Mode: This value determines the access to Biometric Devices that users in this policy will have.

All Biometric Devices and Clients: Users in this policy have access to all Biometric Devices and all Clients for MSO Identification.

Per User: Users in this policy will have access to the Biometric Device(s) specified in the User Distribution Groups selected for them in User Management and cannot be overridden. The same will take place for Clients when using MSO Identication.

© Refer to End User License Agreement for Copyright Notice

Checking the Allow MA 500 database selection during user enrollment allows you to choose the section of an MA 500 where you want to add your user. The MA 500 must have an extended license for 50k users. When adding a new user you will have a drop down menu of zero to four. This is were you decide which of the five sections of the database you want to add the user to.

Time Mask Mode:

24 Hours, 7 Days a Week: No Time mask is specified. All users have access to selected Biometric Devices and MSO Identification Clients at all times.

Custom: Users in this group only have access to the Biometric Devices and MSO Identification Clients during the times specified in the time mask for this policy and cannot be overridden.

Extended User Details: If enabled, additional user information such as Phone Number(s), Email, and Address can be entered for a user.

Wiegand Profile: Select the Wiegand Profile you wish to use for users in this User Policy.

The Wiegand Profile you choose for your users should match the one you utilize for your biometric access devices set in the Biometric Device Profile section of this manual.

User Authentication Mode: Designate the authentication mode you wish to utilize for user placed into this User Policy.

Finger Biometric Enrollment Minimum Fingers: Designate the minimum number of fingers that will be captured during user enrollment. Options are None, One, Two, Three,(with third as the Duress Finger), and Ten.

Preferred Finger One: Designate the first preferred finger for capture on the Finger Biometric Enrollment wizard screen of User Management.

Preferred Finger Two: Designate the second preferred finger for capture on the Finger Biometric Enrollment wizard screen of User Management.

Preferred Duress Finger: Designate the Durress Finger to be captured on the Finger Biometric Enrollment wizard screen of User Management.

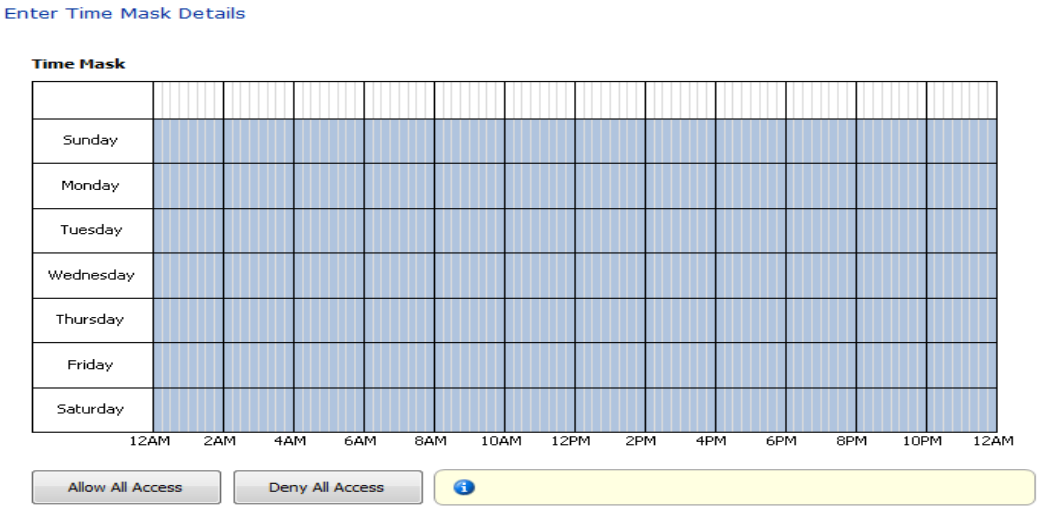
Durress Finger can only be utilized on the Morpho Sigma family of readers.

© Refer to End User License Agreement for Copyright Notice

Screen 2 – Time Mask

The time mask allows you to create access times by selecting from the table with 15 minute steps across 24 hours for each day of the week.

Click and drag the mouse over the required areas to select and deselect times. The time area in blue indicates access is allowed. White indicates access is denied. The buttons “Allow All Access” and “Deny All Access” can be used to clear or set access for all days and times.

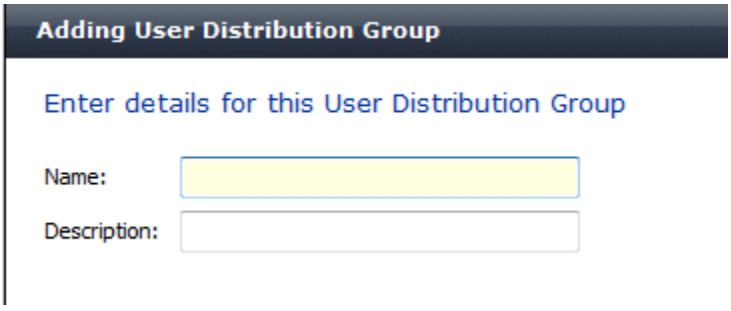


User Distribution Group

User Distribution Groups are designed to distribute users onto groups of MA readers or MorphoManager Clients. In order to be utilized the user must be in a User Policy that has its Access Mode set to “Per User”. Then the User Distribution Groups will be selectable when creating (or editing) a user.

Create a User Distribution Group

Screen 1 – Details



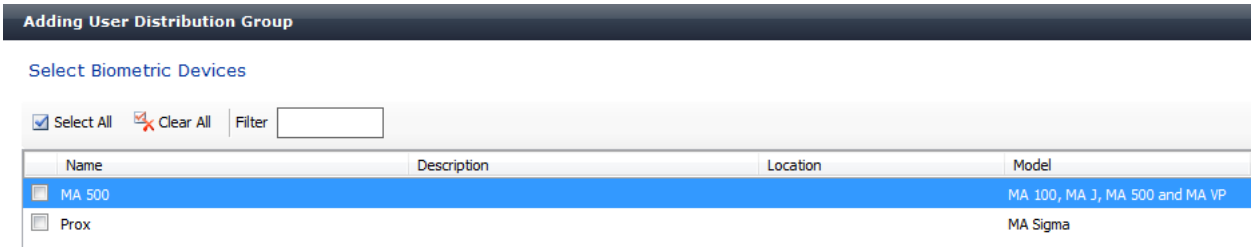
Name: Name of the User Distribution Group

Description: Description of the purpose of the group.

© Refer to End User License Agreement for Copyright Notice

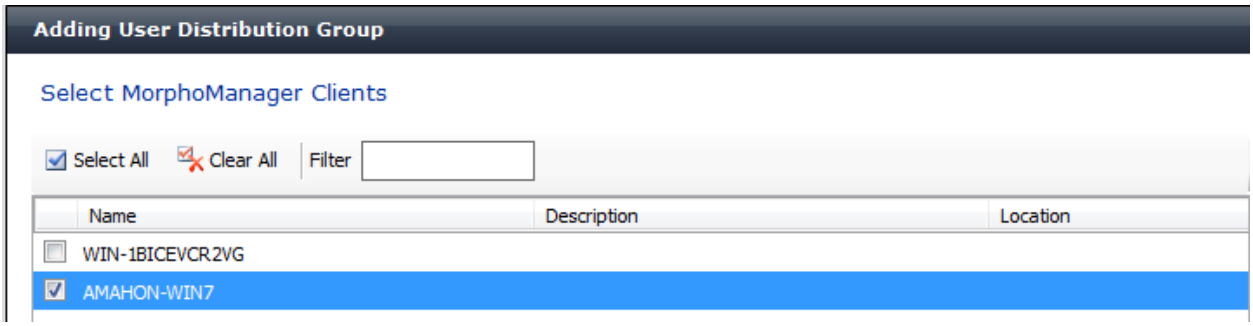
Screen 2 – Select Biometric Device Access

Select the Biometric Device(s) that this group will have access to. The “Select All” button will allow access to all Biometric Devices. The “Clear All” button will remove access to all devices.



Screen 3 – Select MorphoManager Client Access

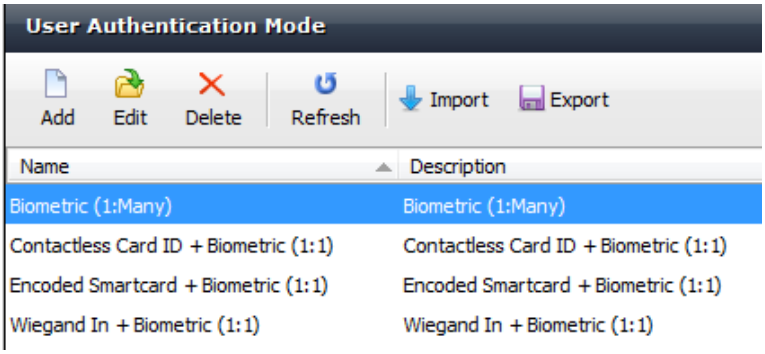
Select the MorphoManager Client(s) that this group will have access to.



User Authentication Mode

User Authentication Mode(s) will set which authentication triggers will be utilized by users. The parameters are designated here and then a specific User Authentication Mode will be chosen as part of a User Policy. Users added to the system will have their authentication triggers governed by the User Authenticatin Mode portion of the User Policy they are placed in.

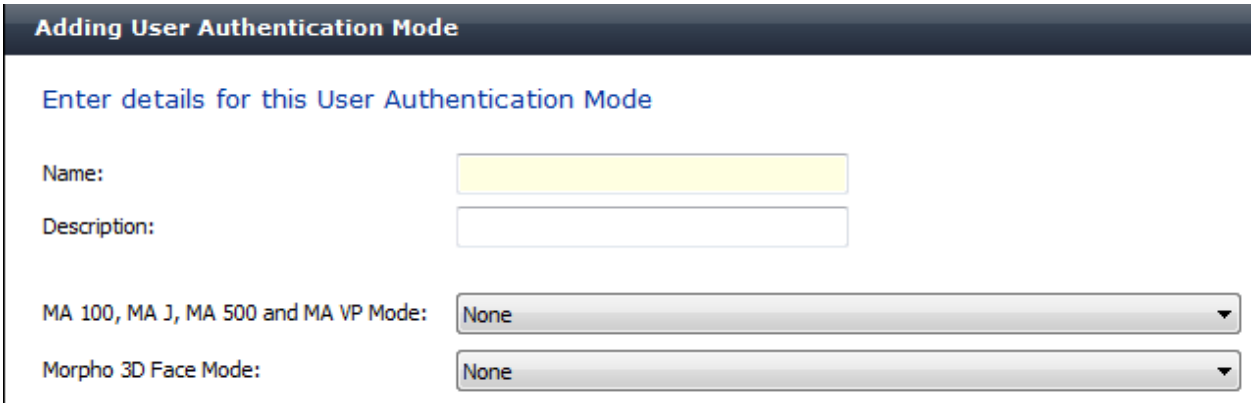
There are four automatically generated User Authentication Modes:



© Refer to End User License Agreement for Copyright Notice

Create a new User Authentication Mode

Screen 1 – Details, MA 2G Family Mode, and 3D Face Mode



Name: Name of the User Authentication Mode.

Description: Description of the purpose of the mode.

MA 100, MA J, MA 500, and MA VP Mode : Select None or the desired authentication mode from the dropdown menu.

Identifier Template Downloaded to Device: The user is authenticated by presenting their finger at a Biometric Device and matching with fingerprint data stored on the Biometric Device. Or, they can key in their authentication identifier at the device and then present their finger.

Identifier Template Encoded to Smartcard: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the fingerprint scanner is activated. The user is authenticated by presenting their finger at the Biometric Device and matching with fingerprint data stored on the card.

Identifier PIN Encoded to Smartcard: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the keypad is activated. The user is authenticated if the PIN code entered matches the stored PIN code.

Identfier Template PIN Encoded to Smartcard: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the keypad is activated. If the PIN code entered matches the stored PIN code the fingerprint scanner is activated. The user is authenticated by

© Refer to End User License Agreement for Copyright Notice

presenting their finger at the Biometric Device and matching with fingerprint data stored on the Biometric Device.

Identifier Encoded to Smartcard: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. The user is authenticated if the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device.

Identifier Encoded to Smartcard Identifier Template Downloaded to Device: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the fingerprint scanner is activated. The user is authenticated by presenting their finger at the Biometric Device and matching with fingerprint data stored on the device.

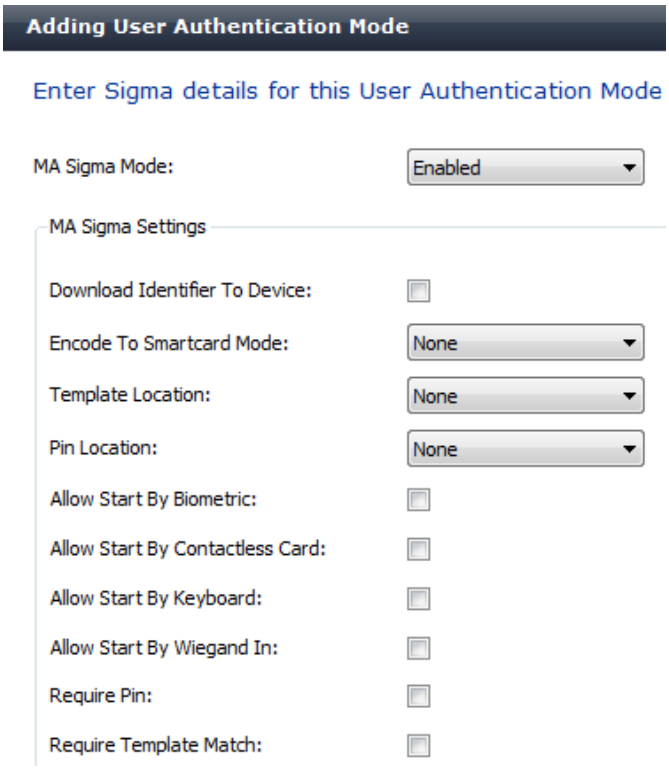
Identifier From Smartcard IdentifierTemplate Downloaded to Device: The user carries a card with a Card Serial Number (CSN) Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the fingerprint scanner is activated. The user is authenticated by presenting their finger at the Biometric Device and matching with fingerprint data stored on the device

Morpho 3D Face Mode :

Identifier Template Download to Device: The user is authenticated by presenting their face at a 3D Face Reader Biometric Device and matching with 3D Face data stored on the Biometric Device.

© Refer to End User License Agreement for Copyright Notice

Screen 2 – Details for MA Sigma mode



MA Sigma Mode: Can be left as None if you are not utilizing MA Sigma devices**.**

Download Identifier To Device: Will download the users Wiegand Code to the MA Sigma.

Encode to Smartcard Mode:

Allow: Will allow smartcard coding for a user, but will not prompt during user creation.

Allow and Prompt: Will allow smartcard encoding for a user and will prompt to encode the card during user creation.

Template Location:

Download to Device: Will download users biometric template onto the MA Sigma.

Encoded to Smartcard: Select when you want to encode user's biometric template onto a smartcard.

PIN Location:

Downloaded to Device: Will download users PIN onto the MA Sigma.

Encoded to Smartcard: Select when you want to encode the user's PIN onto a smartcard.

© Refer to End User License Agreement for Copyright Notice

Allow Start by Biometric:	Allow the trigger for authentication to be started by presenting the user's finger to the Sigma.
Allow Start by Contactless Card:	Allow the trigger for authentication to be started by presenting the user's smartcard to the Sigma.
Allow Start by Keyboard:	Allow the trigger for authentication to be started by touching the keyboard screen icon on the Sigma.
Allow Start by Wiegand In:	Allow the trigger for authentication to be started by receiving a Wiegand In signal to the Sigma.
Require PIN:	Makes using a PIN mandatory for authentication.
Require Template Match:	Makes using correct biometric template for user authentication.

Operator Role

Creating and modifying Operator roles is an advanced feature that should only be used by experienced operators.

Screen 1 – Operator Roles Details

Enter the name for this operator role.

Screen 2 – Custom Commands

Select the custom commands this operator role will allow execute access to.

Screen 3 – Entity Access

Select the entities this operator role will have access to and the type of access (view, add, edit, delete, import, export).

Screen 4 – Report Access

Select the reports this operator role will have access to.

Screen 5 – User Interface Access Set

Select the user interface elements this operator will have access to.

© Refer to End User License Agreement for Copyright Notice

Clients

Clients are computers that have the MorphoManager Client software installed and communicate with a MorphoManager server.

Screen 1 - Client Details

Name: Name of the computer the client is installed on.
Description: A description of the purpose of the client.
Location: The physical location of the client computer.

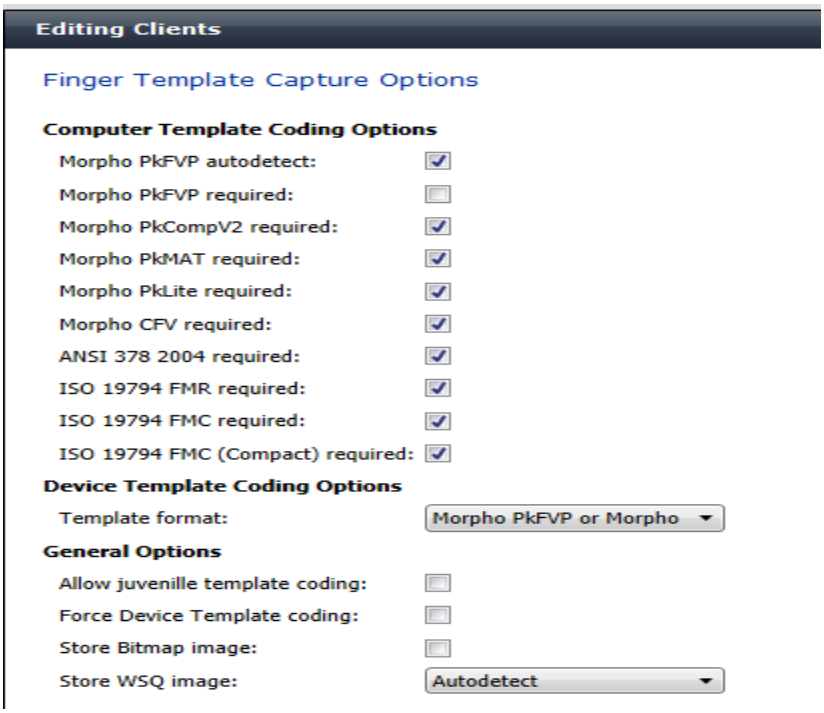
Screen 2 - Tabs

Select the tabs that are displayed on this client. MorphoManager will need to be closed and restarted for the changes to take effect.

Screen 3 - Camera Configuration

Setup the camera that is connected to this client.

Screen 4 - Finger Template Capture Options

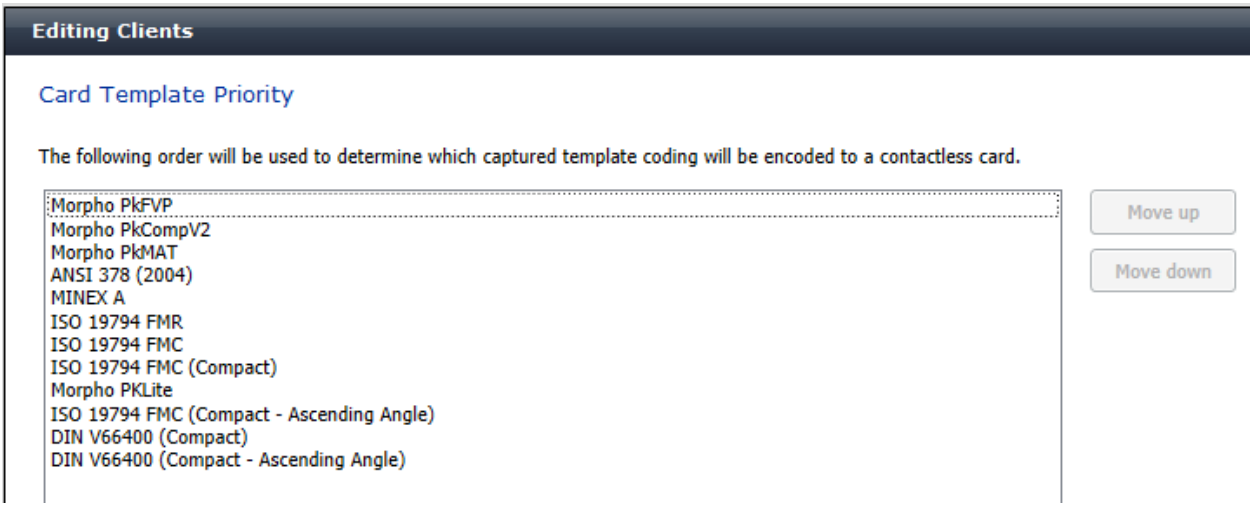


Computer Template Coding Options: configures the template formats that will be coded when an enrollment is performed using MorphoKit.

© Refer to End User License Agreement for Copyright Notice

Device Template Coding Options: configures the (single) template format that will be coded when an enrollment is performed using MorphoSmart.

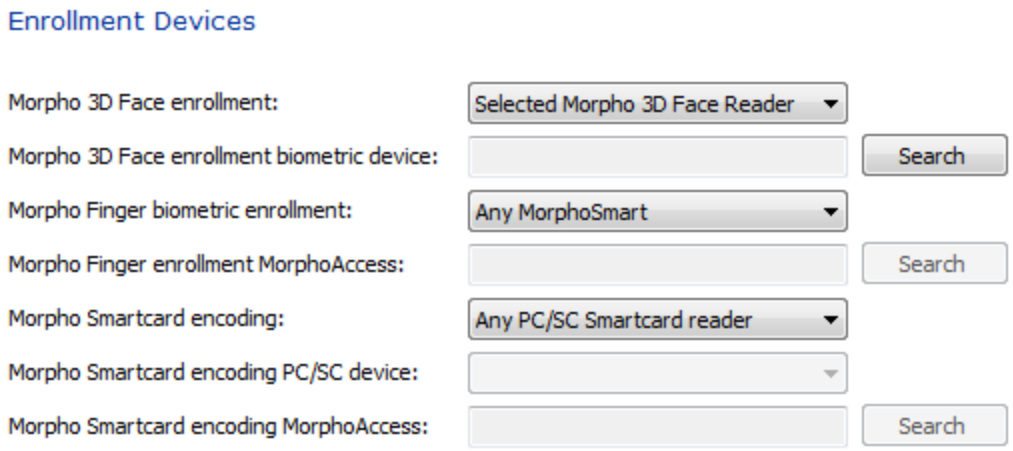
Screen 5 – Card Template Priority



Screen 6 - Enrollment Devices

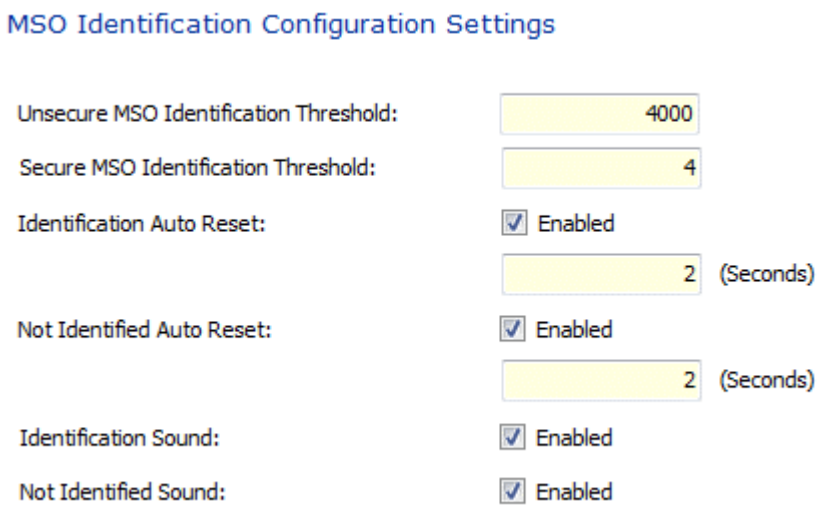
Select the Enrollment Devices you wish to utilize in MorphoManager during User enrollment. You can specifiy any MorphoSmart device to use the first detected MorphoSmart for finger enrollment, or alternatively select a specific device (if more than one is attached to this PC) or use a selected MorphoAccess Sigma device for enrollment.

For card encoding, you can select any PC/SC device to utilize the first detected device, a specific PC/SC device (if more than one is present) or elect to use a selected MorphoAccess Sigma for card encoding (only on MA Sigma Multi and MA Sigma iClass).



© Refer to End User License Agreement for Copyright Notice

Screen 7 – MSO Identification Configuration Settings



Unsecure MSO Identification Threshold: This value specifies the threshold score for positive identification on Unsecured MSO devices. By default, the score should be set to 4000. Lowering the score will reduce the security, but allow users with lower quality fingerprints to be identified. Raising the score will increase security, but users with lower quality fingerprints may not be identified.

Secure MSO Identification Threshold: This value determines the identification threshold for Secured MSO devices. The default value for this setting is 4 (1-10). Lowering the score will reduce the security, but allow users with lower quality fingerprints to be identified. Raising the score will increase security, but users with lower quality fingerprints may not be identified.

Identification Auto Reset: If enabled, specifies the amount of time (in seconds) to display the "Identified" screen prior to returning to presentation mode.

Not Identified Auto Reset: If enabled, specifies the amount of time (in seconds) to display the "Not Identified" screen prior to returning to presentation mode.

Identification Sound: If enabled, a sound will be played via the computer's speakers indicating a positive identification has occurred.

Not Identified Sound: If enabled, a sound will be played via the computer's speakers indicating a not identified event has occurred.

© Refer to End User License Agreement for Copyright Notice

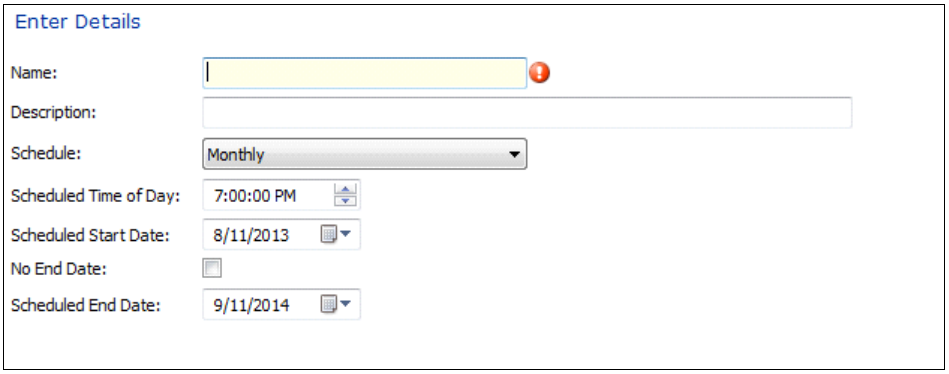
Scheduled Reports

Scheduled reports enable the periodic generation and delivery of reports based on a predefined set of criteria.

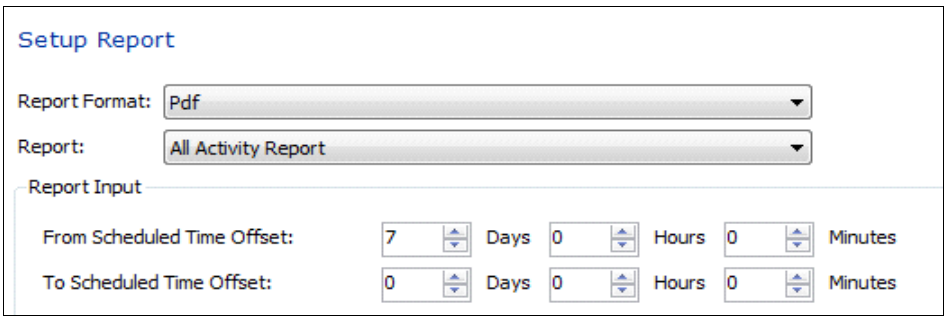
SMTP Settings must be configured in system configuration before a scheduled report can be created.

To add a new scheduled report, click the **Add** button.

Fill in the details for the scheduled report and click **Next**.



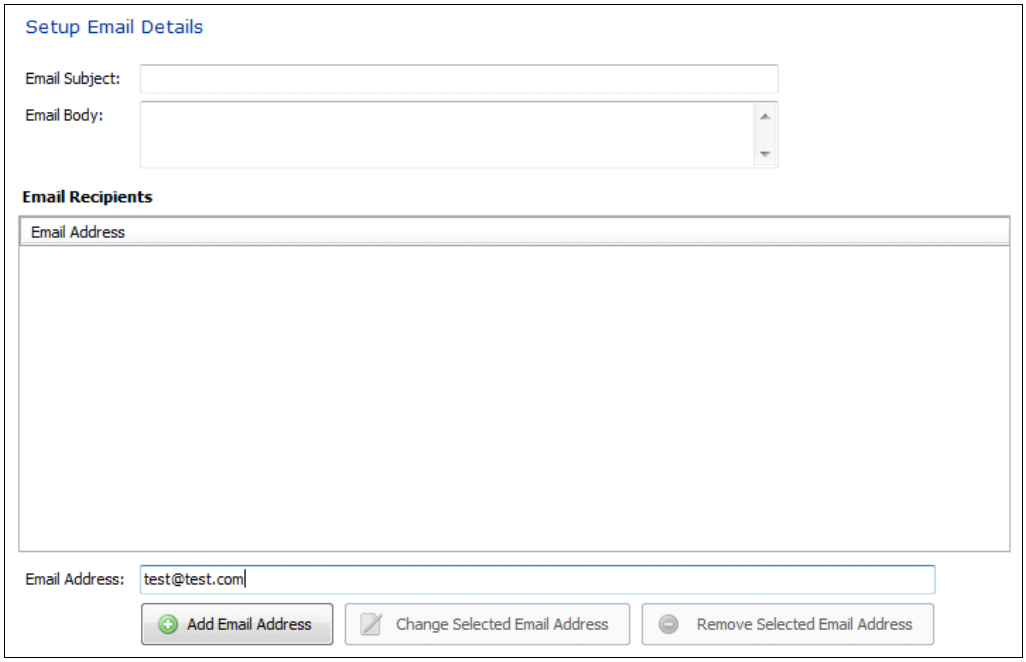
Select the format of the scheduled report. Options are pdf, word document, or excel spread sheet.



Select the type of report that will be generated and enter the details for that report type. The scheduled report will use those details each time it automatically generates a scheduled report. Some report types allow for an offset to be entered. This allows reports to be generated for a specific date range relative to the current date e.g. A report can be set to run every week for the last seven days.

Click **Next** to go to the next page when the details are correct.

© Refer to End User License Agreement for Copyright Notice



Enter the email subject, body of the email and the recipients.

To add a recipient, type the email address in the text box and click **Add Email Address**. To edit an existing email address, select the address to change, type in the new address and click **Change Selected Email Address**. To remove a recipient, select the email address and click **Remove Selected Email Address**. This information will be used whenever this scheduled report is generated. Click **Finish** to save the scheduled report.

To change the details of the selected scheduled report, click on **Edit** in the toolbar. To remove the selected scheduled report, click on **Delete**. To generate the selected scheduled report now instead of waiting for the predefined generation interval, click on **Run Report Now**.

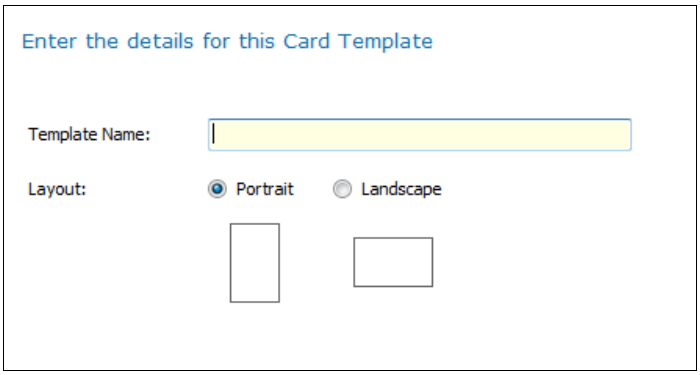
© Refer to End User License Agreement for Copyright Notice

Card Template

A card template is used to print ID cards for enrolled personnel.

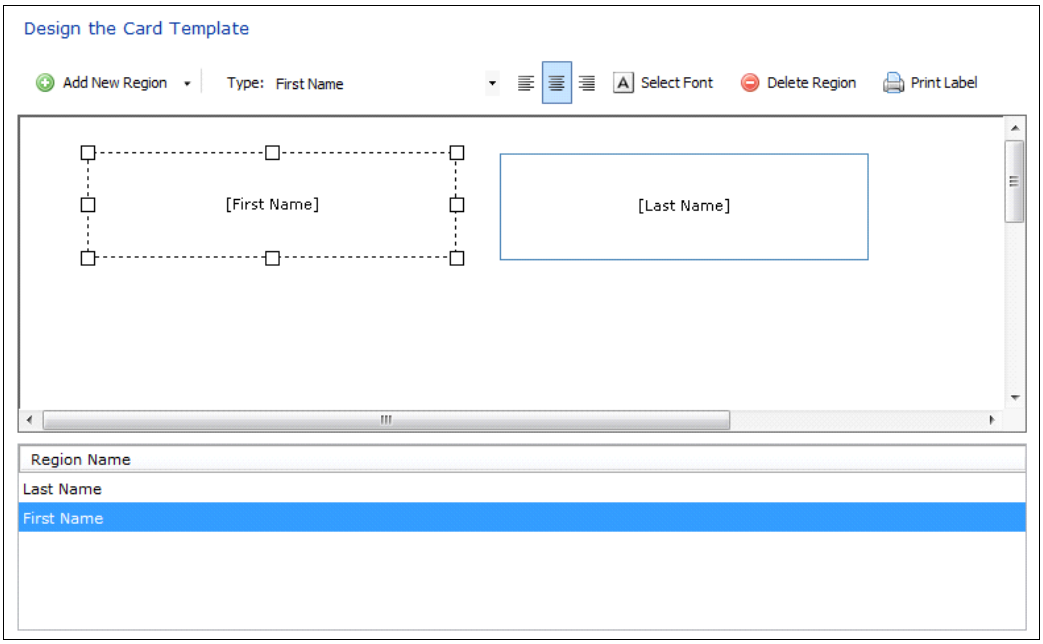
Screen 1 - Details

Enter a name for the template and select the layout of the card.



Screen 2 - Design

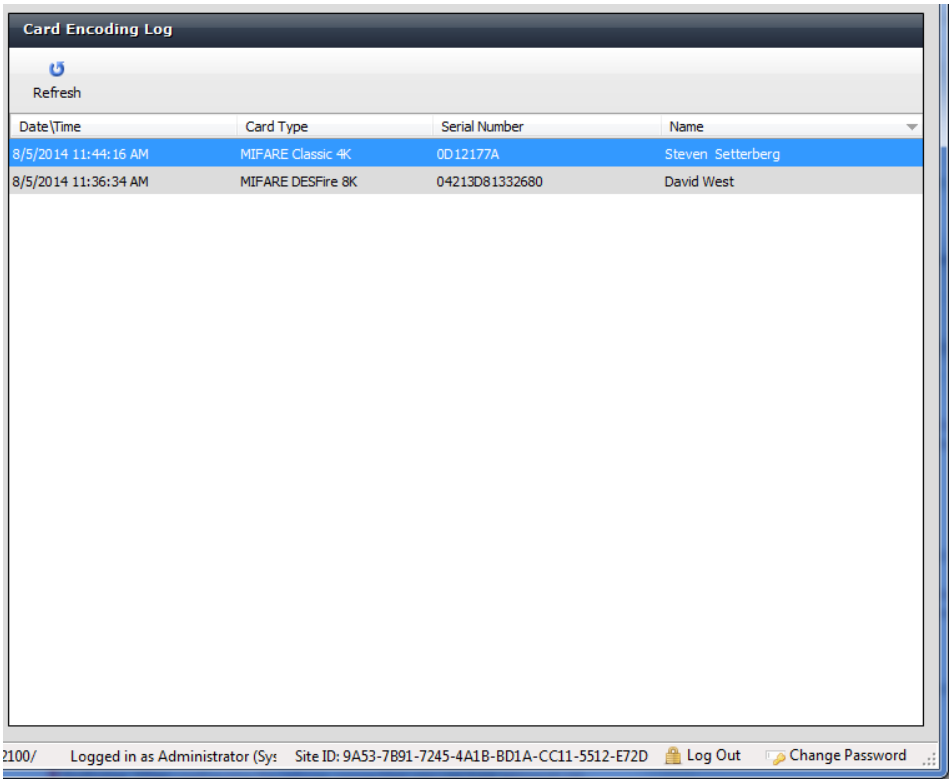
Use this screen to design the layout of the card. A region is an item that can be moved around and will be replaced by the actual data when the card is printed (e.g. First Name). A background image can also be added for logos or artwork that is required on the card. To edit a region, click on it or select it from the list below, and change the options using the toolbar items. The region's alignment (left, center or right), font and type can be changed. The size of the region can be changed by dragging the boxes on the edges of the region. To change a background image region, select the region and click **Load Image**. To remove a region, select it and click **Delete Region**.



© Refer to End User License Agreement for Copyright Notice

Card Encoding Log

This area is designed to store a log of all smartcards encoded via MorphoManager. Informatation will include the Date\Time stamp, the Card Type, Serial Number, and user name. The user name will be shown as Unknown if the user has been deleted from the system.



Event Logs

Here you will find the history of internal actions performed by MorphoManager. A common error is a failed attempt by MorphoManager to communicate with the Biometric Device. This situation will occur if, for example, there is more than one Biometric Device and all are in error – this may well point to the network hub being switched off or if power to all Biometric Device has been interrupted.

A **Send to Support** button is available when discussing an error with the support team. You may be asked about the information on the screen and also asked that the log be emailed to support for further analysis. When clicked, the log file is automatically attached to a new email using the default email client on the PC. Where it can be examined by support staff to help determine the process needed to rectify any fault conditions.

The “export logs” action is useful for a situation where the MorphoManager PC is not connected to the Internet, allowing the file to be saved in a location for future reference. To export event logs, click on **Save to Disk** button and save it in the location needed. The last selection allows for the start and end date and times to be selected. Select the destination for the file and click **Save**.

© Refer to End User License Agreement for Copyright Notice

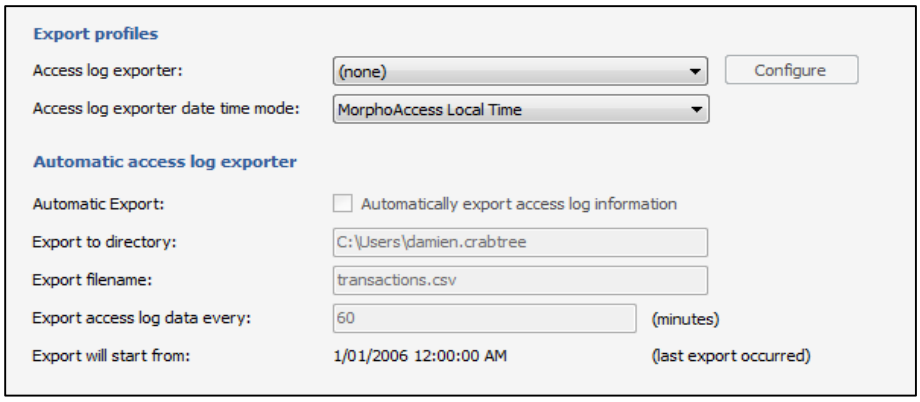
Exception Logs

Exception logs store messages that are created by MorphoManager in the event of an internal action not producing the expected results.

The Export Logs and Email Logs to Support icons provide the same functionality as previously outlined in event logs.

System Configuration

Section 1 – Time and Attendance



Access Log Exporter

These setting are used for manual and automatic access log exporting to a Payroll or Rostering software package. You need to select the format you want the exported data to comply with. You may choose from ASTROW, Commac, Preceda, Timeminder, Powerforce, RosterOn, MYOB , MorphoManager Standard, Kronos, Pay Global (Employee ID/Wiegand Usercode), Sodb and TimeAmerica.

Automatic Access Log Exporter

Click on the tick box for **Automatic export access log information** and select a destination for the exported file.

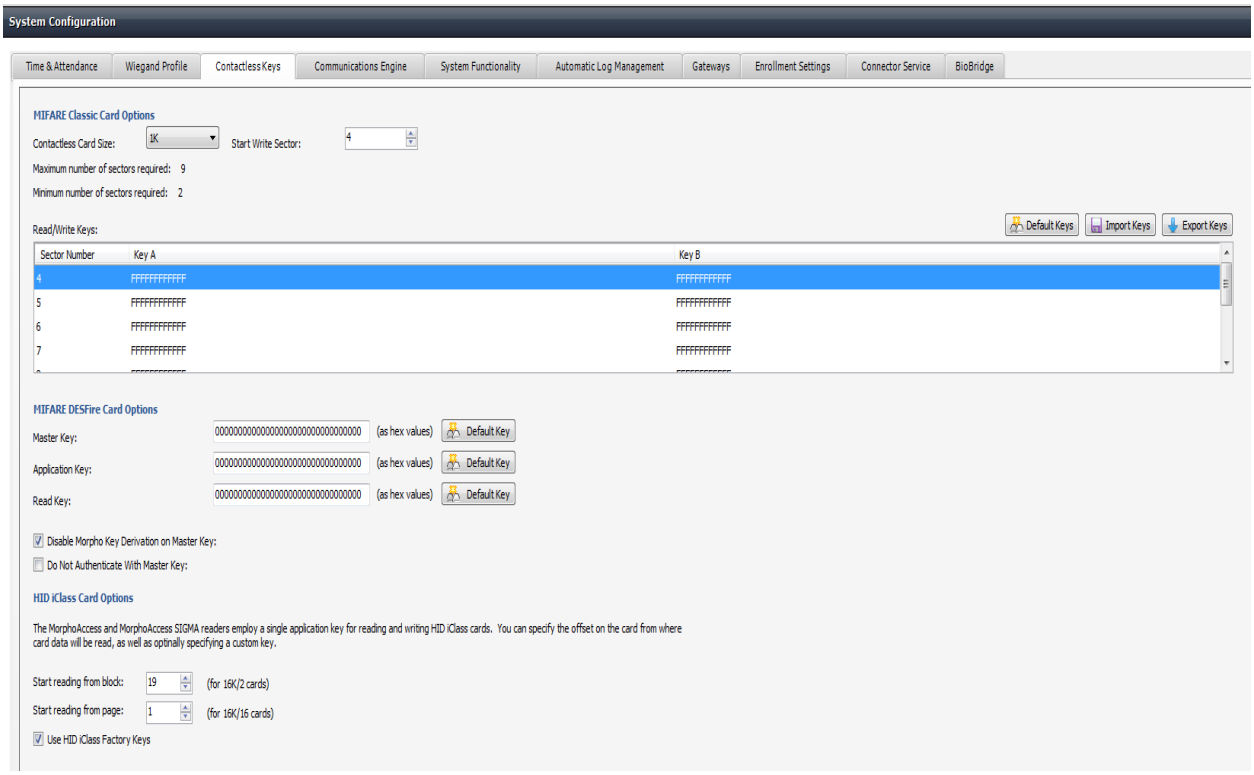
Enter the default file name and destination for the file. The directory MUST exist on the server computer as the file will be saved to the server's hard drive.

The file will be exported at the interval specified at **Export access log data every**.

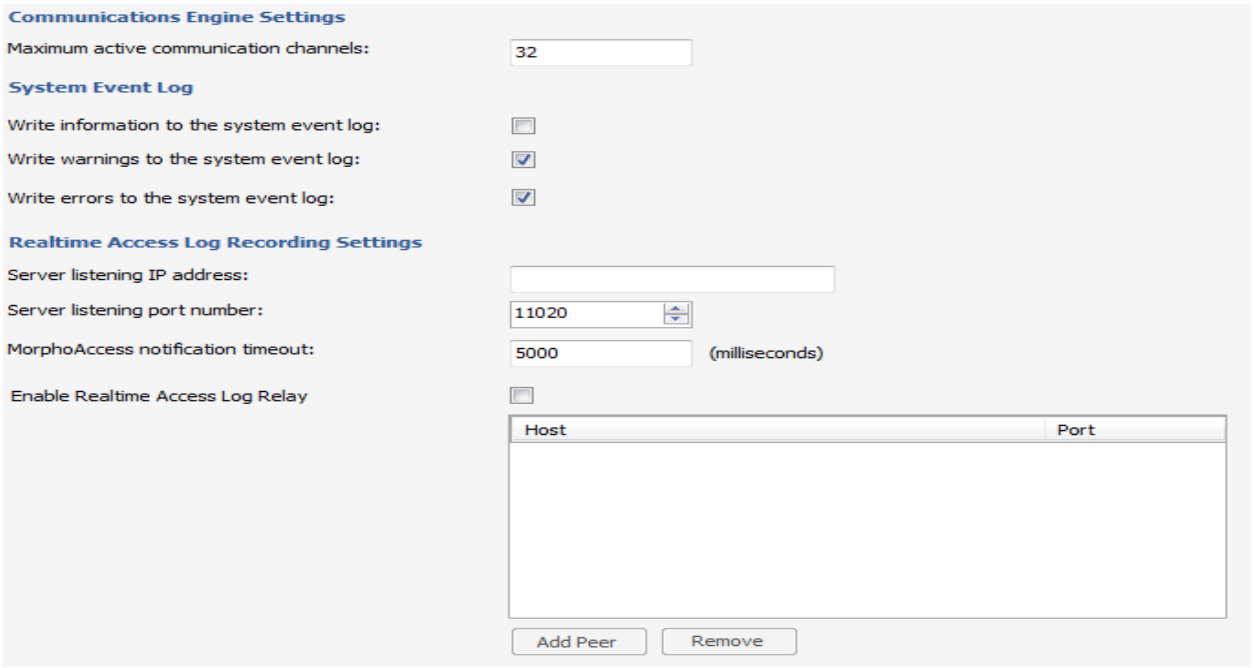
© Refer to End User License Agreement for Copyright Notice

Section 2 – Contactless Keys

Contactless Keys can be set for MIFARE Classic, MIFARE DESFire, and HID iClass cards.



Section 3 – Communications Engine



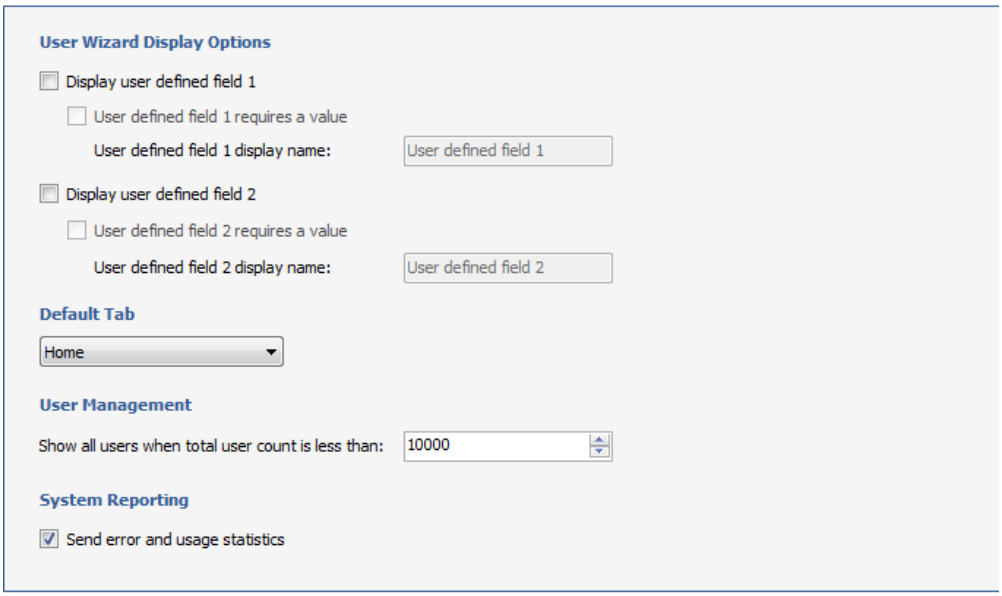
© Refer to End User License Agreement for Copyright Notice

Maximum Active Communication Channels: The maximum number of active communication channels.

System Event Log: Select the types of information to write to the system event log.

Real-time Access Log Recording Settings: These settings are to be configured to use the Real-time Access logs for a Biometric Device.

Section 4 – System Functionality



Display extended User details
In user details by default only the first of two pages are presented during enrollment and display. The second page allows entry of additional information such as Phone Number, Fax Number, Mobile Number, Email and Address details.

Display user defined field 1 (and 2)
Selecting this option displays another page in the wizard that collects the information from these fields. Select the fields to display, whether or not information is mandatory and the names of the fields to display.

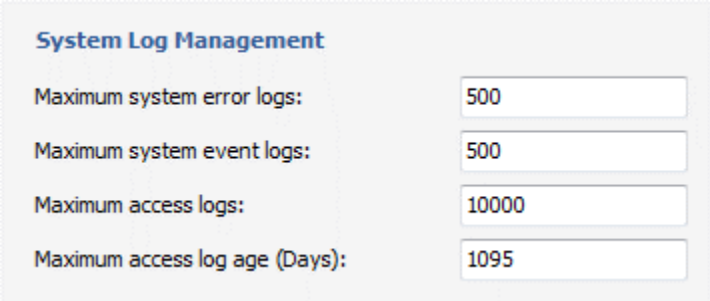
User Policy Display Name
The name entered here is used instead of "User Policy" in all areas of MorphoManager.

Default Tab
This defines the tab selected by default when MorphoManager starts.

User Management
This allows you to control how many users will appear on your User Management screen. If you have more than the amount in the value filed, you can use filtering to find the additional users.

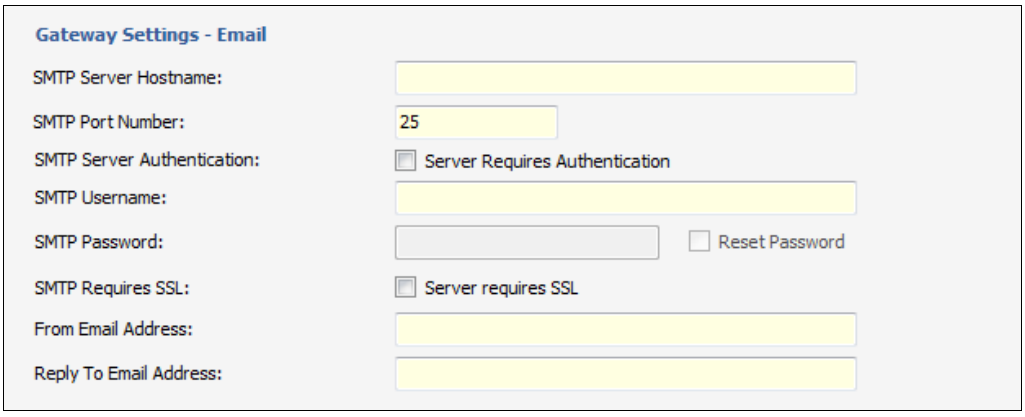
© Refer to End User License Agreement for Copyright Notice

Section 5 – Automatic Log Management



These settings are in place to prevent any log files from becoming unmanageable due to their size. The above values are the default values. When the log count reaches these values the oldest logs are deleted until they are within the values specified.

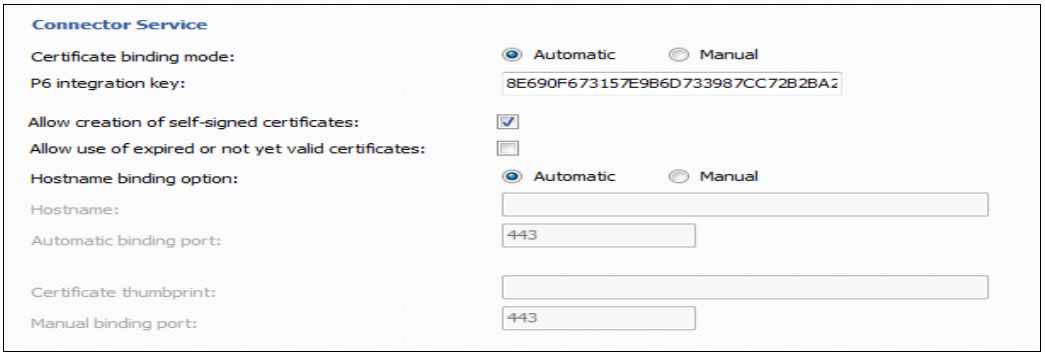
Section 6 – Gateways



The Gateway settings are used to receive emails for Scheduled Reports. These settings are specific to the Mail server. For further assistance to configure the gateway settings, please refer to your IT support.
Automatic Certificate Binding Mode.

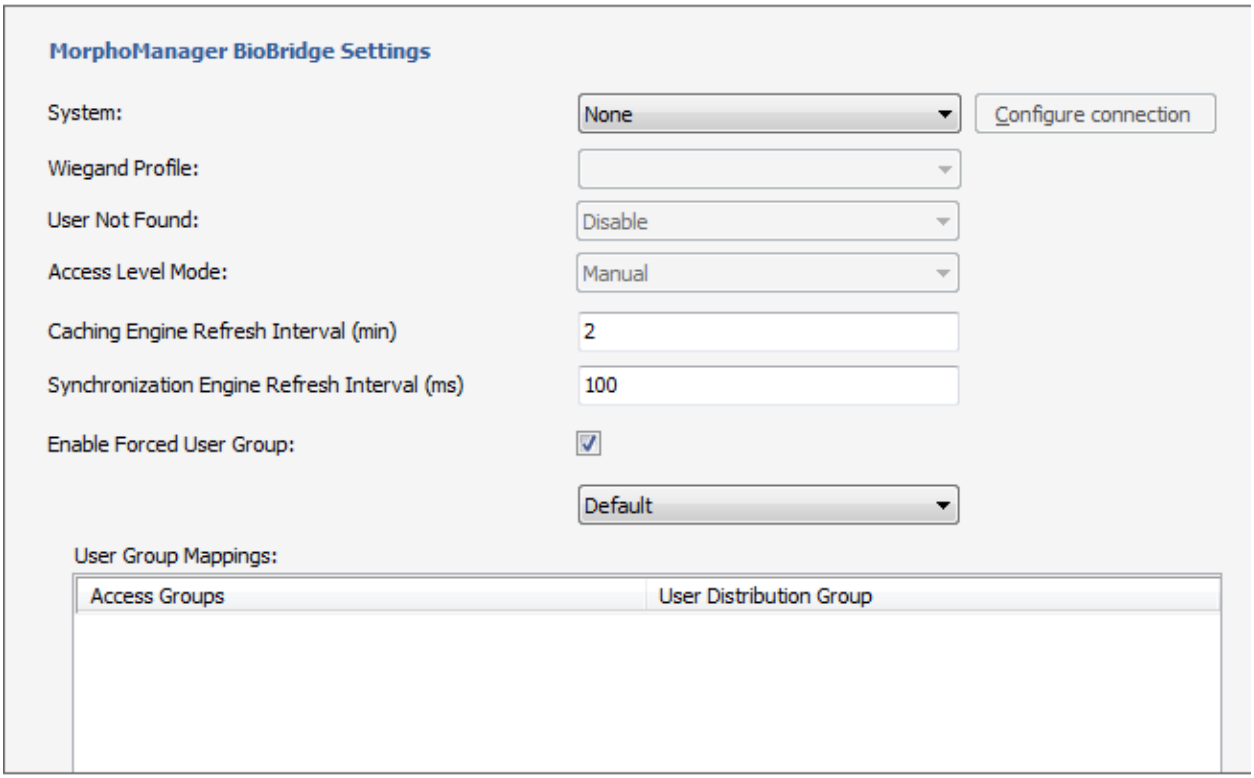
Section 7 – Connector Service

Enter the settings for the connector service.



© Refer to End User License Agreement for Copyright Notice

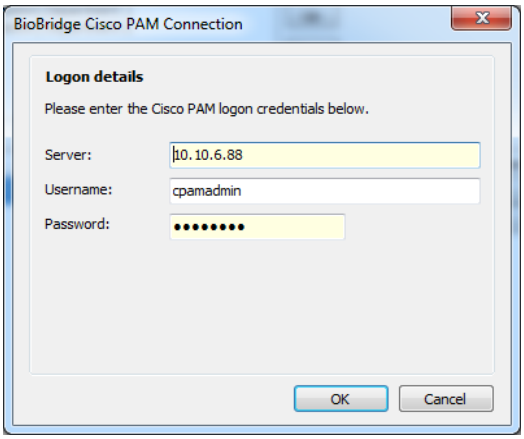
Section 8 – BioBridge



Completely optional, BioBridge allows you to extract user data from compatible third-party systems. User/grouping Information can be "synced" by the BioBridge Enrollment Client when you set the configurations for the respective third-party system. You can set "rules" for when data is synced between both parties. One example would be by disabling or deleting enrolled users that were not already enrolled in the MorphoManager client itself.

System
Choose your BioBridge compatible system from the drop down menu.

Configure connection
Connection credentials for the third-party software.



© Refer to End User License Agreement for Copyright Notice

Wiegand Profile
Most (but not all) BioBridge compatible systems use a specific Wiegand format to identify users/cardholders. This can be specified on Cards, Card Types or can be specified as a "Wiegand Format". Please select the Wiegand format in use from the drop down menu.

User Not Found
This setting determines what action MorphoManager should take when a previously enrolled user is not found in the BioBridge system.

Access Level Mode
This setting determines how MorphoManager should map BioBridge users into MorphoManager User Distribution Groups. This can be done by either automatically trying to map based on the names (Automatic), or by manually selecting which BioBridge Access Level maps to which MorphoManager User Distribution Group.

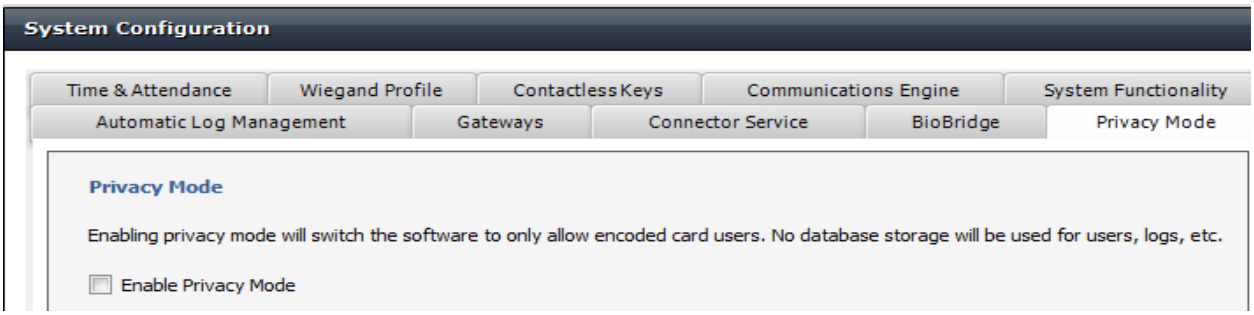
Enable Forced User Policy
By activating this feature you can select a User Policy from the drop down menu. The 3rd party user will automatically be placed in this User Policy during the enrollment process started in the BioBridge Enrollment Client. The User Policy selected here must be a "Per User" access mode policy.

User Policy Mappings
This displays and allows for modification of how the BioBridge groups map to MorphoManager User Distribution Groups (if using Manual Grouping Mode). If no MorphoManager User Distribution Group is selected for a particular BioBridge Grouping, those users will not be available for enrollment into MorphoManager.

For more details, please refer to the separate BioBridge Quick Start Guide manuals for specific vendors.

Section 9 - Privacy Mode

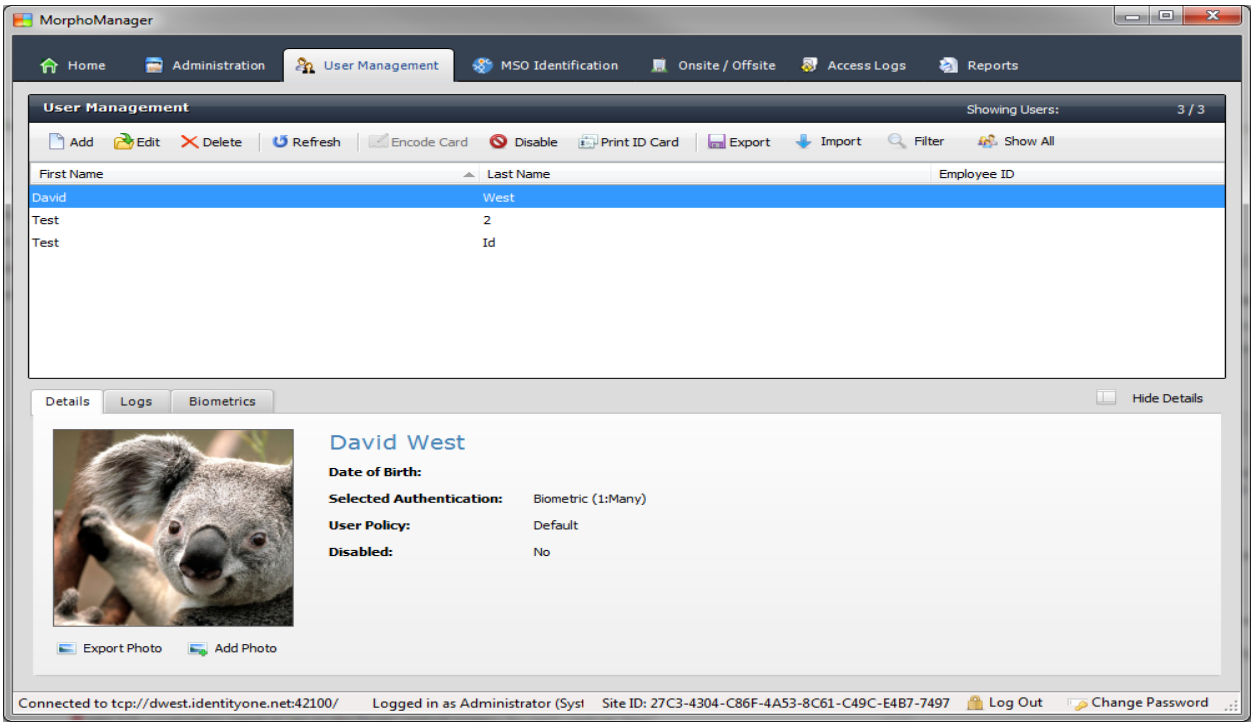
This mode will allow customers to enroll card-only users (i.e. Card-only, Card + PIN, Card + Fingerprints, Card + Fingerprints + PIN) without saving their details to the MorphoManager database. This mode will apply to all User Policies, and will only apply to **new** enrolments. Users who are enrolled in this mode will not appear in User Management. Additionally, if Privacy Mode is enabled log retrieval will be disabled.



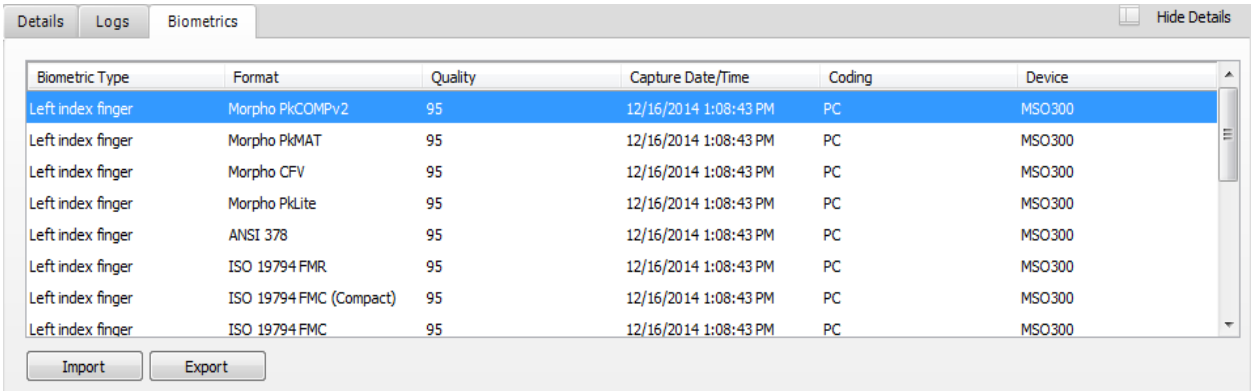
© Refer to End User License Agreement for Copyright Notice

User Management

Users are people who will have their biometric data (or minutia) sent to the selected Biometric Device for identification purposes for either access control or time and attendance. Select the user management tab to access this area.



Select any user to view the details and logs of the user in the bottom details area. Detailed information about the enrolled fingers can be viewed on the Finger Biometrics Tab. Fingerprints can be exported from this tab.



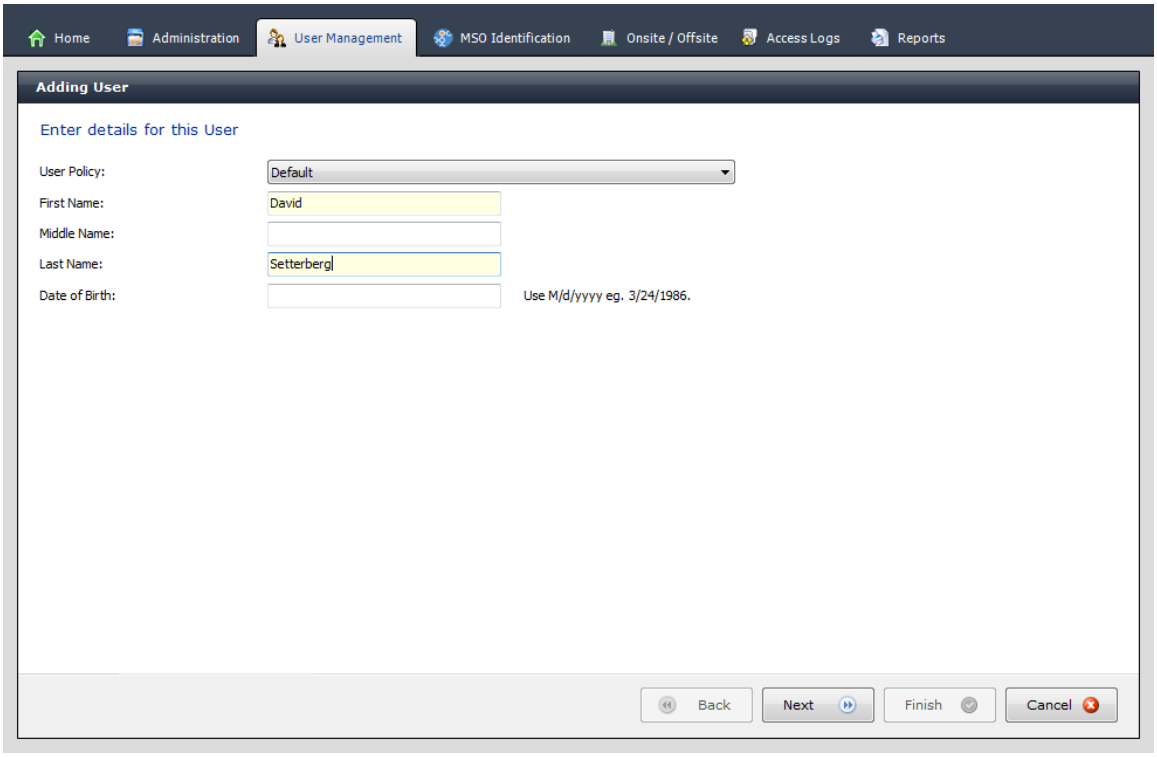
Creation and enrollment of a User

To create a new user, select the click the **Add** button on the Toolbar. This will display the User Wizard.

© Refer to End User License Agreement for Copyright Notice

Screen 1 – User Details

Enter the details for the new user.



User Policy: Select the User Policy that this user will belong to. This is an important selection, as the policy will determine Biometric Device access and other access control and time & attendance settings.

First Name: User's first Name **(Required)**

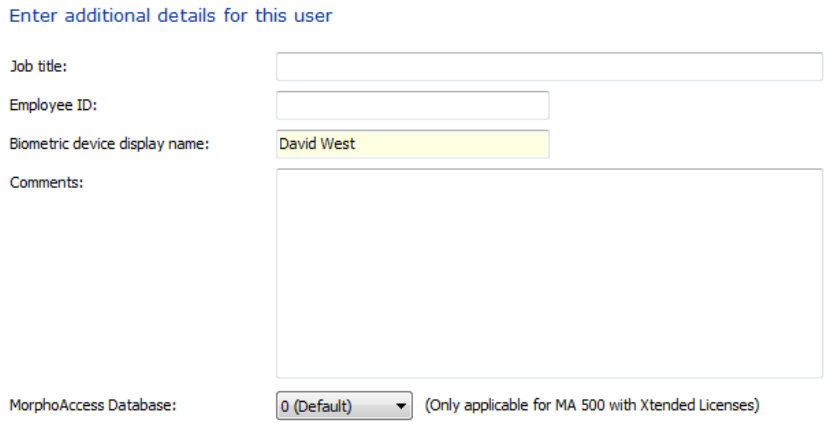
Middle Name: User's Middle Name

Last Name: User's Last Name **(Required)**

Date of Birth: Enter the date of birth of the user. This can be entered in several different ways. E.g. 30th May 1975 could be entered in the following ways 30/5/75, 30-5-75, 30 May 1975, 30 5 1975.

© Refer to End User License Agreement for Copyright Notice

Screen 2 – Additional Details



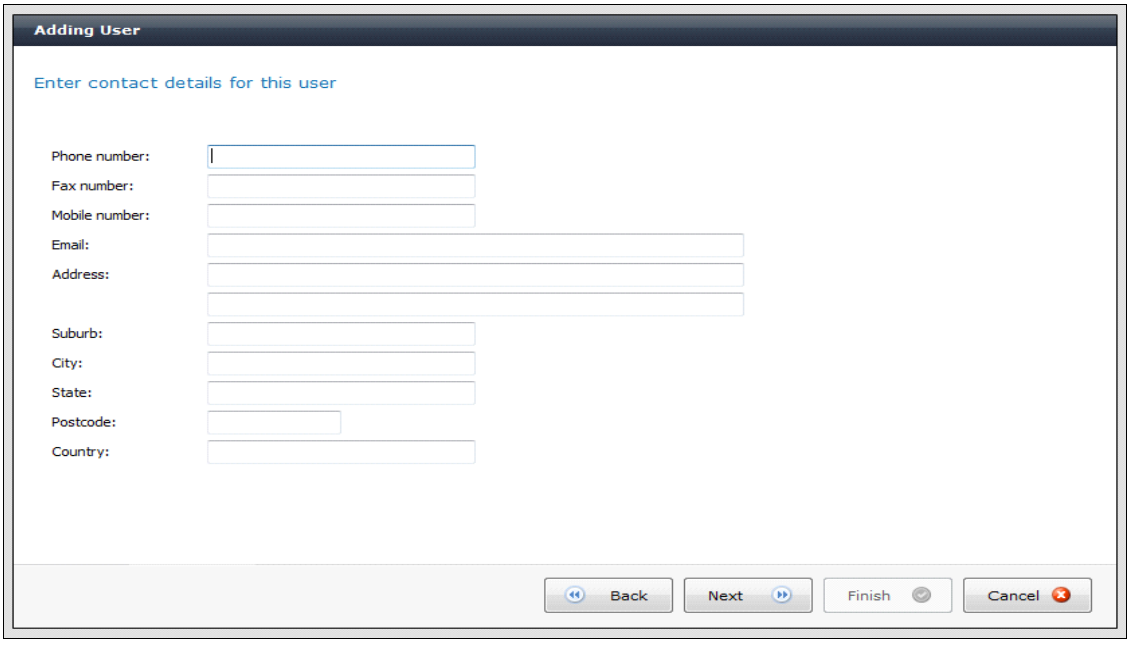
Job Title: The user's job title.

Employee ID: A company specific code that may be assigned to a user. If used for "Time and Attendance", this field should match the employee number from the Payroll or Rostering software.

Biometric Device Display Name: The information displayed upon acceptance by the Biometric Device and defaults to the First and last name of the user.

Comments: Any additional information that is relevant to that person.

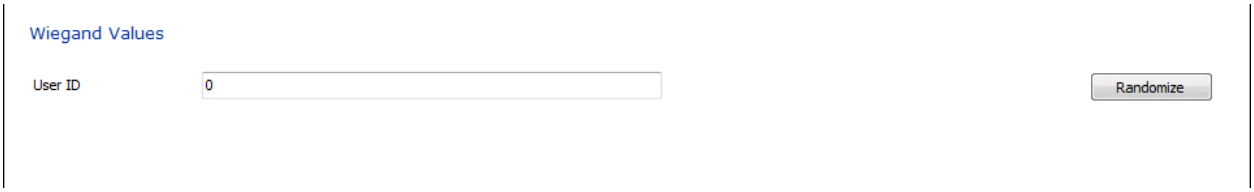
Screen 3 – Contact Details



© Refer to End User License Agreement for Copyright Notice

This page is only visible if “Display Extended user policy details” has been enabled on the selected User Policy. If so, enter the details for the selected user.

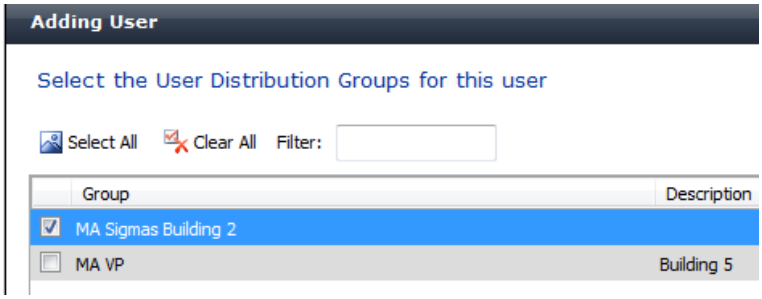
Screen 4 – Biometric Device Override Details (If a Wiegand Profile is set)



The User ID can be put in manually or by utilizing the Randomize button. This screen is only available if you have changed the User Policy to have a particular Wiegand Profile set, rather than leaving the default setting of “Automaticially generated random 64 bit”. Addtionally, a Read Card Serial Number button will be present if you utilize one of the Weigand Profiles referencing Card Serial Numbers.

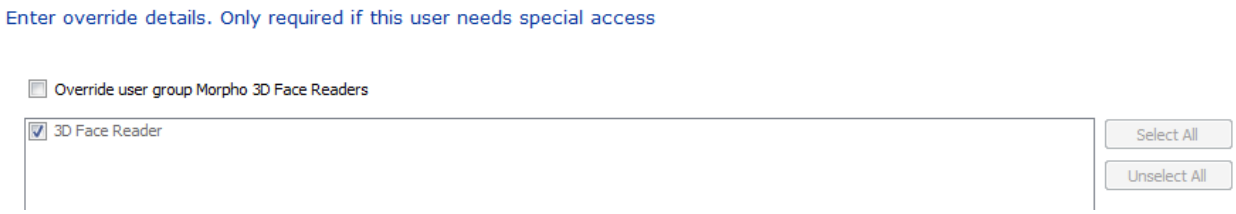
Screen 5 – User Distribution Groups

If your User Policy is a Per User access mode you will be able to select the group of biometric devices you want to place the user on.



Screen 6 – Morpho 3D Face Reader Override Details

This screen is only visible if the Morpho 3D Face Reader access mode is set to “User Policy and User” or “User Only” on the selected user group.

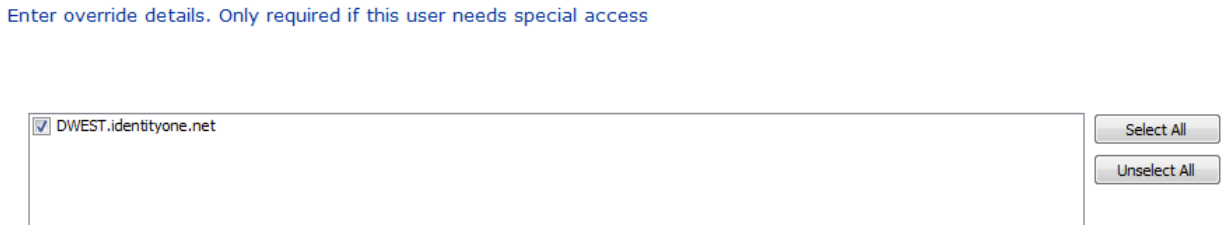


The settings in this form will only be used if the user requires special access that is different from the Morpho 3D Face Reader that was specified in the User Group. Check the “Override user group Morpho 3D Face Readers” and select the Morpho 3D Face Reader(s) this user will be enrolled on.

© Refer to End User License Agreement for Copyright Notice

Screen 7 – MSO Identification Client Override Details

This screen is only visible if the MSO Identification Client access mode is set to “User Group and User” or “User Only” on the selected user group.



The settings in this form will only be used if the user requires special access that is different from the MSO Identification Client that was specified in the User Group. Check the “Override user group MSO Identification Client” and select the MSO Identification Client(s) this user will be enrolled on.

Screen 8 – Photo Capture

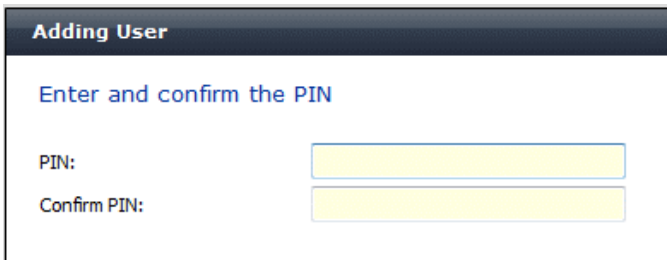
Position the person in front of a plain background so that all of their face is visible in the picture, similar to a passport photo. Once the user is positioned correctly click **Capture Photo**. Click on the image in the top left corner and drag towards the bottom right drawing a square around the part of the photo to keep. This can be done many times until the correct area is selected. Click **Accept Changes** to accept the changes if no camera is connected just click **Next**.

If the person is not available to have their photo taken, click **Person not at Camera**, to skip photo capture.

© Refer to End User License Agreement for Copyright Notice

If the photo is not acceptable, click **Update Photo** to recapture the photo. Photos can be imported and exported using the corresponding buttons. Additional configuration options for the camera can be changed by clicking on **Configure Camera**.

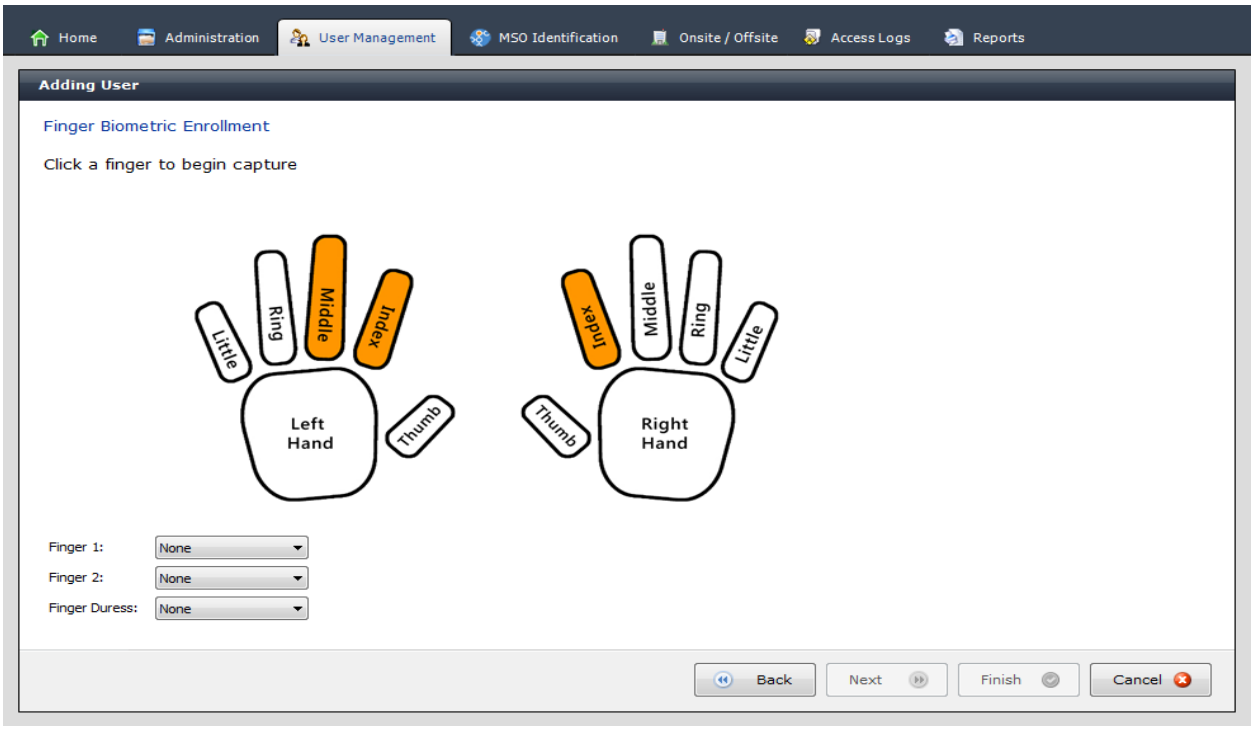
Screen 9 – PIN Code



PIN Code: Will be utilized and appear on screen when the authentication mode is set to one including PIN. Ex. Smartcard + PIN.

© Refer to End User License Agreement for Copyright Notice

Screen 10 – Fingerprint Capture

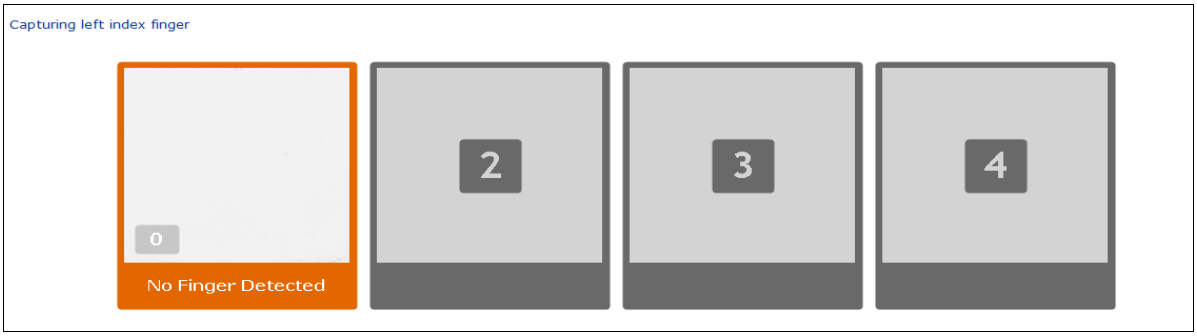


The default fingers that the system suggests you to enroll are set at the User Group level and are flashing orange. **You do not need to use these fingers as you can click on others. However, you will need to set Finger 1 and Finger 2 from their respective drop downs lists after fingerprint capture.**

If either of the following conditions occurs a “No Device” message box will be displayed when you select a finger to enroll:

- There is no fingerprint reader connected
- The fingerprint reader connected is the wrong model for the software.

If the reader is connected correctly the following screen below will be displayed.



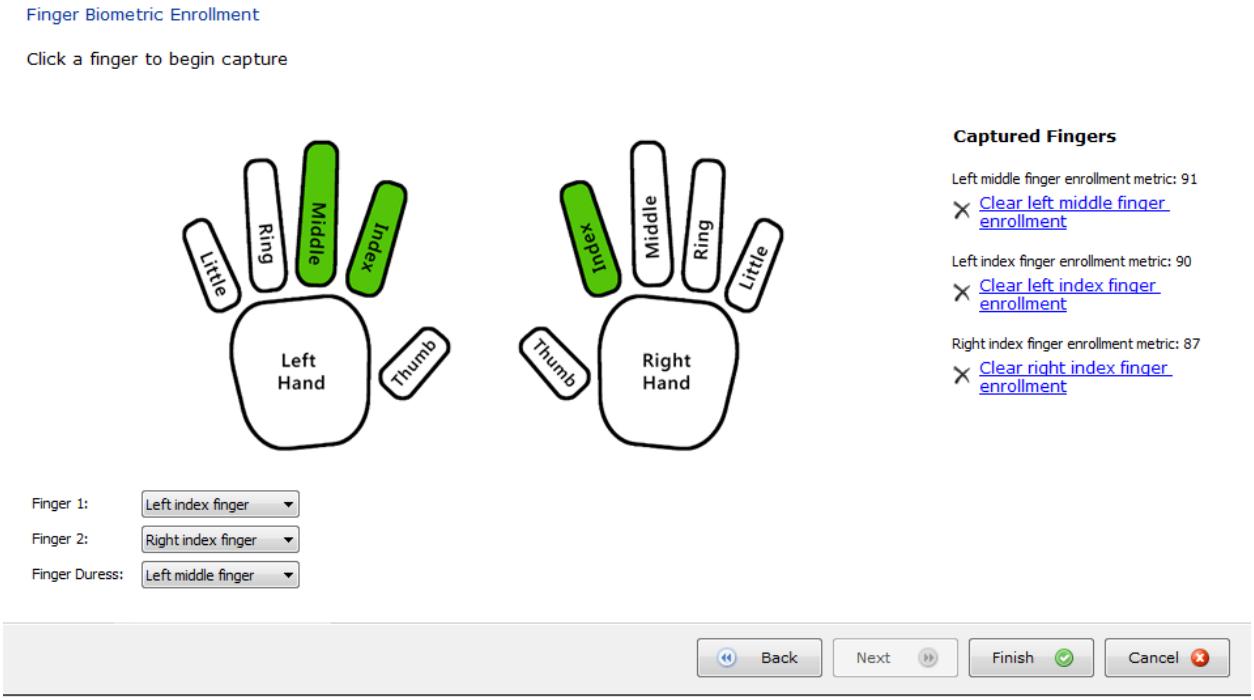
Click on a finger and have the user place their finger in the center of the scanner glass. You will then see the print appear on screen. There are four scans performed on each finger; the first three are used to

© Refer to End User License Agreement for Copyright Notice

create the biometric template. The system selects the best elements of each print and consolidates those features, allowing a greater range of presentations to be recognized. The fourth print is used for verification purposes. Below each enrollment image a color bar will be displayed indicating the quality of the print as it is being captured. Green indicates quality is above recommended quality. Orange indicates the quality is above the minimum but below the recommended quality. Operators with administrative rights are permitted to accept fingerprints of this quality. Red indicates the quality is below the minimum, the user must re-enroll.

Follow the instructions on screen. Green indicates ready to capture. Orange indicates that a finger is presented but the capture has not finished yet. Check the instructions to ensure the finger is placed correctly. When the border is red, the current finger capture is finished. Continue until all boxes are filled.

Once the enrollment is complete for both the fingers, you will see the screen below (this example is utilizing Duress Finger). Captured finger quality is displayed on the right. In the event a user is not being recognized at any Biometric Device with one or both enrolled fingers, click **Clear <*enrolled finger*> finger enrollment** to allow re-enrollment.



Positive Identification and general performance of MorphoManager is maximized by the quality of the fingerprint captured during enrollment. MorphoManager has been designed to reject poor quality fingerprints; however it is still possible they may slip through.

The key to capturing a high quality fingerprint is to visually look for a clearly presented pattern that is centered and square with the right amount of pressure. Don't hesitate to retry the capture if you are unsatisfied. For assistance refer to the fingerprint capture guide. Click **Finish** to save the user or cancel to discard changes.

© Refer to End User License Agreement for Copyright Notice

To get the best performance from your MorphoManager software and Biometric Device hardware, care must be taken with enrollment of users into the system. Below are examples of fingerprint capture which could result in either false acceptance or false rejection of users at your Biometric Device. We also suggest that the Biometric Device be mounted at a height of approximately 1 meter from the ground. Mounting the Biometric Device at this height will facilitate full finger presentation when using the Biometric Device. Mounting the Biometric Device significantly higher or lower on the wall makes presentation of a full fingertip much more difficult.

Figure 1

This is an example of a finger that has been cleaned of oil by methylate spirit. Very little information is shown on the print to develop the algorithm. This can happen if you use hand wipes or hand cleaners prior to using the Biometric Device. If the hand cleaners are used for infection control or similar requirements, either use the hand cleaner after using the Biometric Device or provide a hand cream solution to replace the natural body oils stripped from the hands.

Figure 2

This is an example of a print where the person being enrolled has used only light pressure and partial presentation of the tip of the finger. The user will have difficulty presenting the same portion of the finger when clocking “On” or “Off” if this is allowed during enrollment. This type of enrollment could

© Refer to End User License Agreement for Copyright Notice

also lead to a significant number of false acceptances which is where a user is identified incorrectly. This is because there is little information in this portion of a fingerprint to develop a good algorithm.

Figure 3

Figure 3 shows the finger being presented in two different places on the enrollment device. The MSO300 or 1300 will actually discard any non-matching prints and average those remaining out of the three presentations. If the third print was in a different place again, the software would either accept one as being a match and use that or reject the enrollment. However matching on two prints isn't as good as three identical prints

Figure 4

In this example the captured finger has a large amount of oil on it and pressure was quite high on the reader lens. This will probably work okay but is not ideal. A user needs well defined ridges and troughs as well as intersection points in the print. These sites are the matching points used to develop the algorithm which is the finger template that subsequent finger presentations are matched against at the Biometric Device.

© Refer to End User License Agreement for Copyright Notice

Figure 5

This is an example of the presentation required for the best possible enrollment by a user. This example has good information like visible ridges and intersection points for development of the algorithm by the enrollment device. A full print is presented to the window and even pressure from the finger. The print should use as much of the finger phalange as possible.

User Actions

There are several additional functions available for user management.

Edit: Opens the already saved user details for viewing or editing.

Delete: Use with caution as the user's details will be permanently deleted. This operation cannot be undone.

Refresh: Refreshes the user list from the database. This will update the display with the most current data.

Disable User: When a user is disabled they no longer have access to any Biometric Device. All access logs and user information is retained for reporting. Disabled users can be enabled at any time.

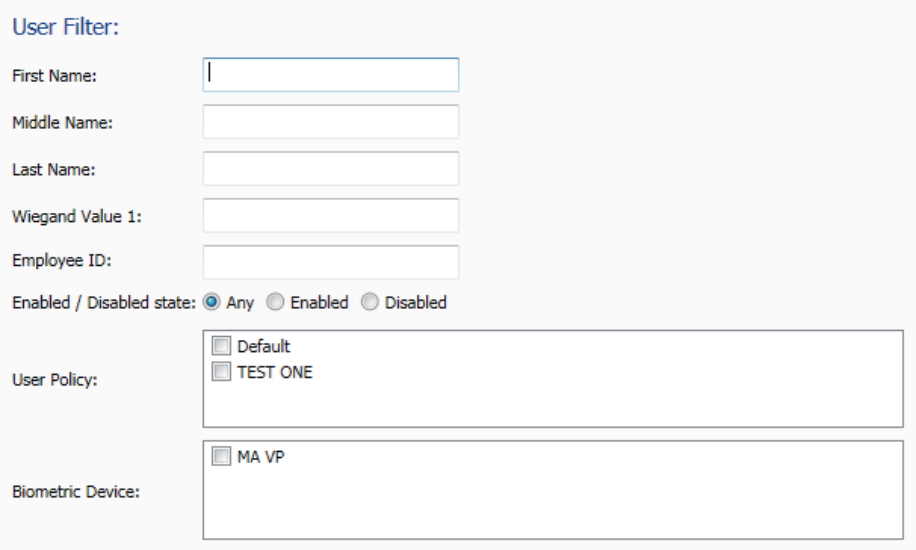
Export Photo: The photo stored in the User record can be saved to disk.

Add Photo: A photo from disk can be used as the user's photo. This is useful if a camera is not connected to the PC.

© Refer to End User License Agreement for Copyright Notice

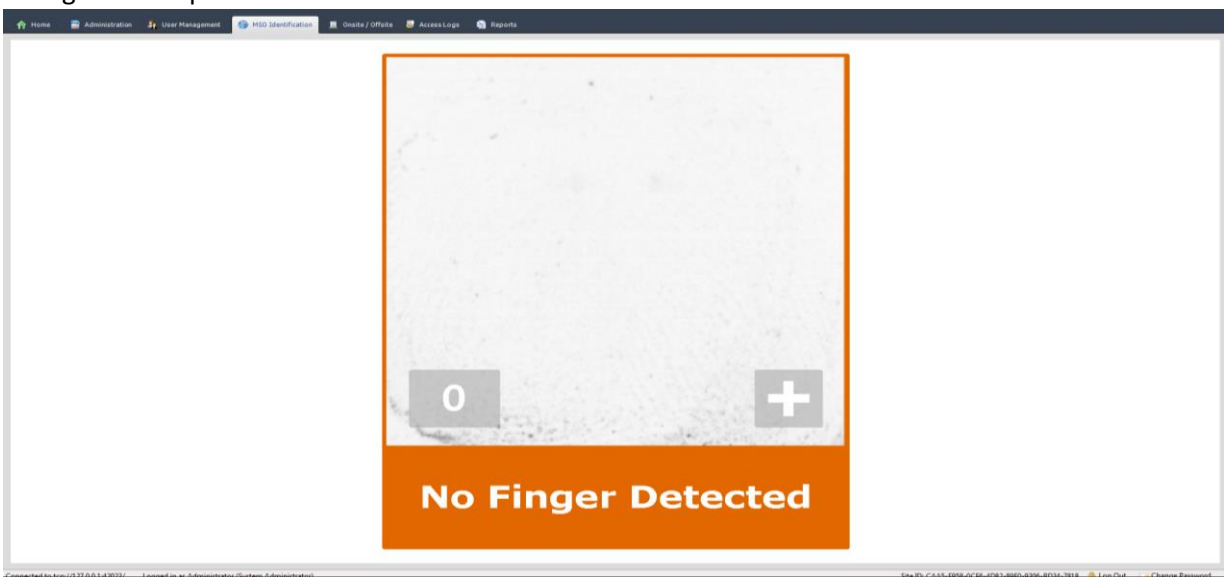
Filtering

The display of users can be filtered by clicking the **Filter** button. Select the required items and click **Ok**. The list of users will automatically be updated using the new filter information. To return the filters to their original state click **Reset Filters**. To display all users click **Show All**.



MSO Identification

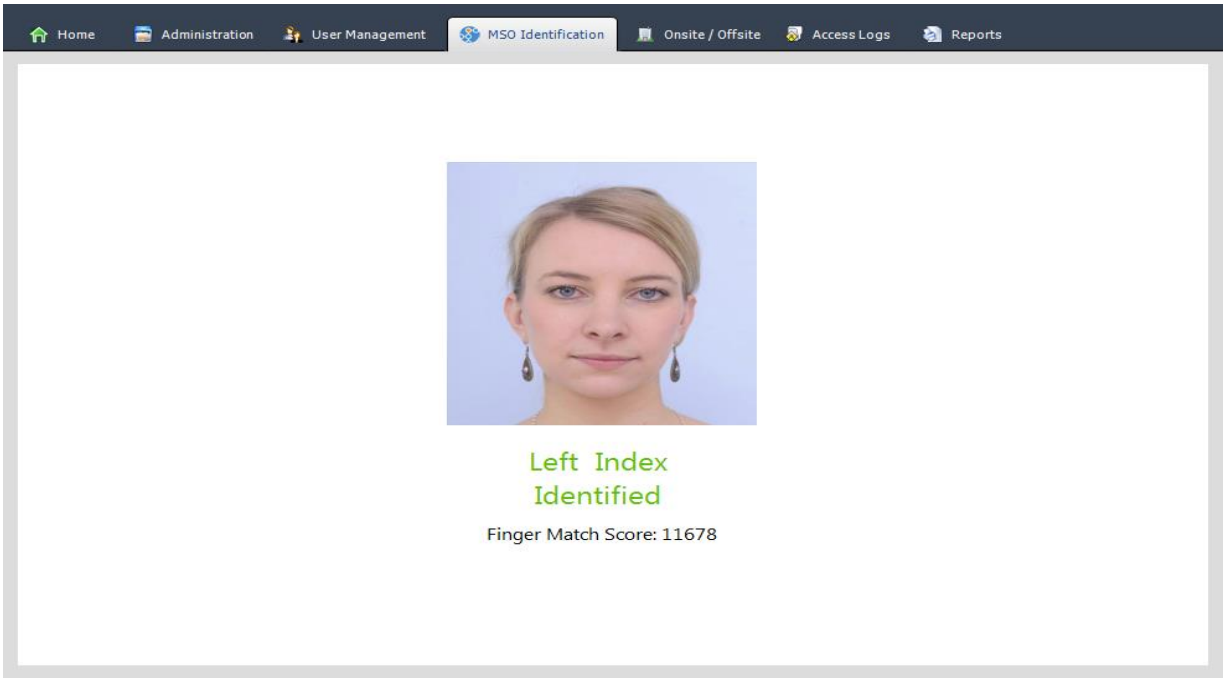
The MSO Identification section allows for users fingerprints to be captured and identified using the configured MorphoSmart device



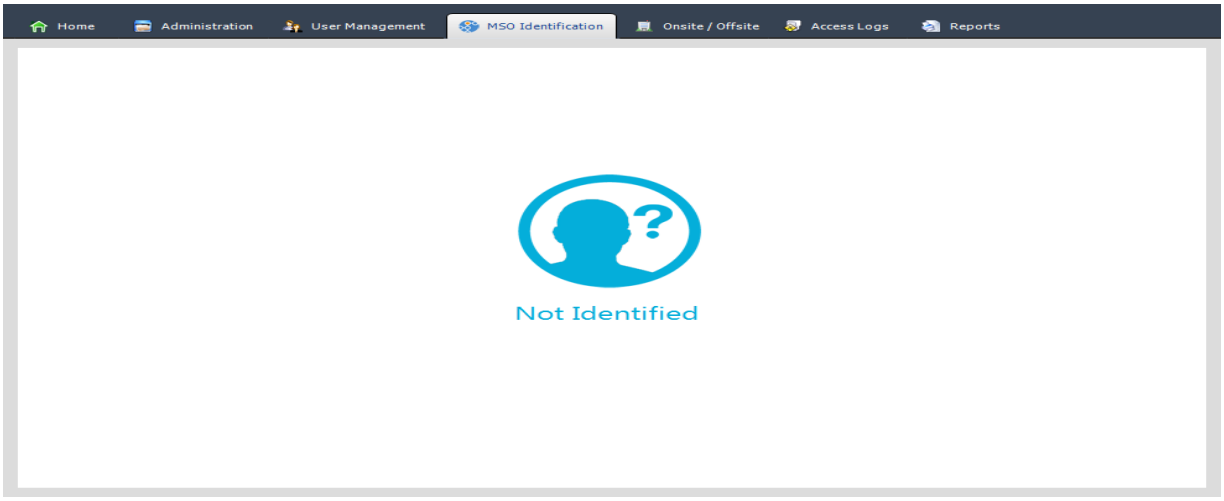
Once the user presents their fingerprint to the MSO device an “Identified” or “Not Identified” screen will be shown.

© Refer to End User License Agreement for Copyright Notice

Identified: The identified user's name, photo and identification score (if using an unsecured MSO device)will be displayed.



Not Identified: If the captured fingerprint is not matched against a previously enrolled finger, the "Not Identified" screen will be shown.



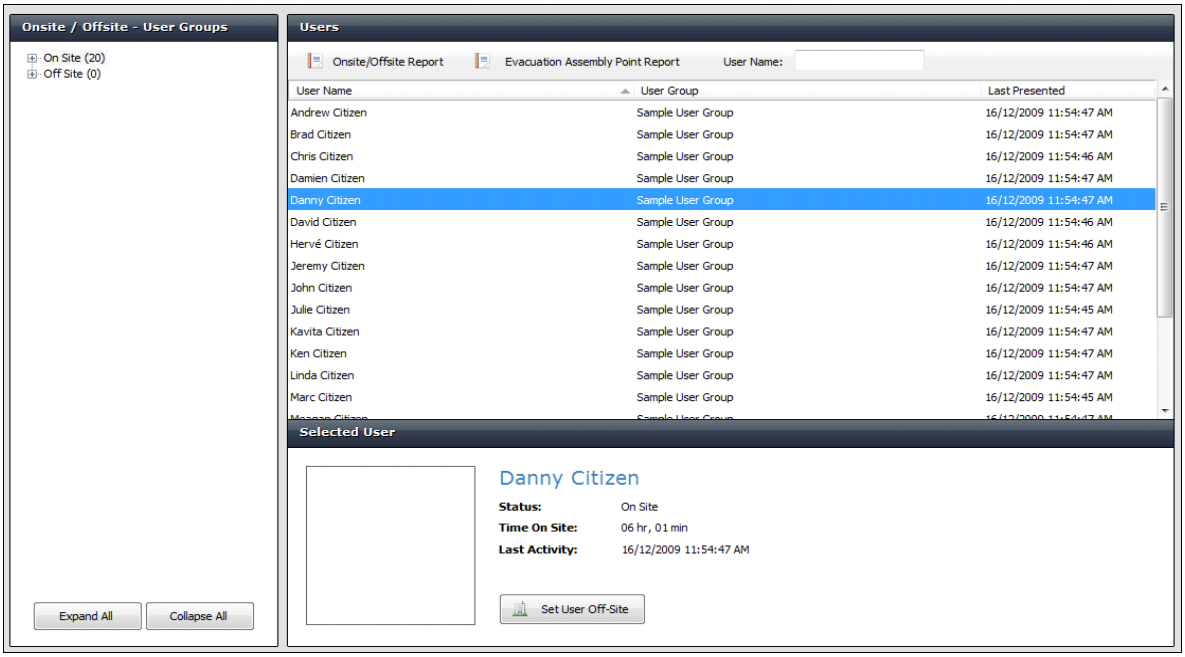
© Refer to End User License Agreement for Copyright Notice

Biometric Device Profile Creation Tool

This tool will allow you to generate a Biometric Device Profile from MA2G or MA5G family parameters that are set on a device. The data will be collected and a file created that can be imported into MorphoManager to utlize as an advanced BDP.

Onsite/Offsite

The Onsite section is used to show which users are currently onsite or offsite. The Onsite and Offsite items in the tree view on the left can be expanded to show user groups.



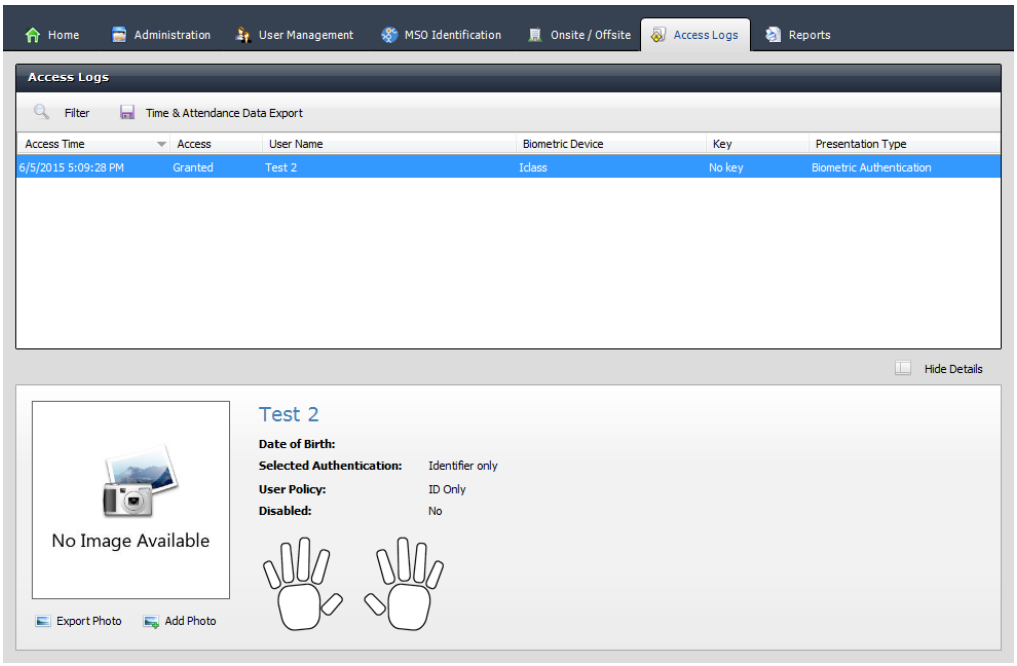
© Refer to End User License Agreement for Copyright Notice

To manually set a user onsite/offsite, click on the User in the Main screen and click on **Set User Off-Site** or **Set User On-Site**.

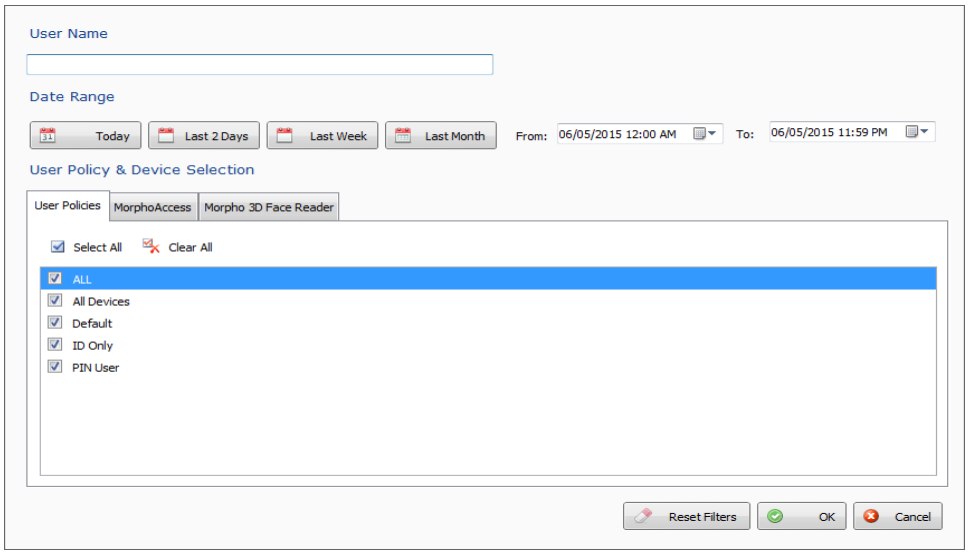
Depending on the Biometric Device Onsite mode that has been set, the users will be shown in onsite or offsite.

Access Logs

An access log is a record of transactions recorded by the system.

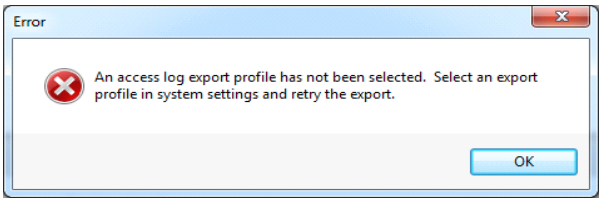


To filter the display of access logs, click **Filter**. Enter or select the details for filtering and click **Ok**. To reset the filters to their original state, click **Reset Filters**.



© Refer to End User License Agreement for Copyright Notice

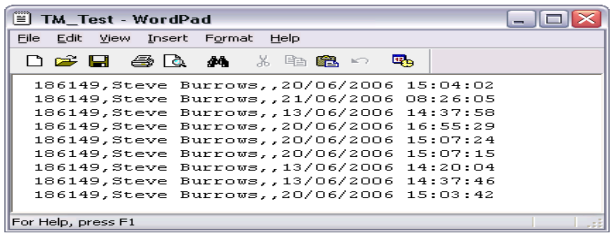
Before the access log can be exported, you need to create an Export profile. This is an initial setup procedure and is performed only once unless you need to export to another type of time and attendance application. The following error will be displayed if the profile(s) have not been created.



Refer to the system configuration section for instructions on configuring an access log export profile.

Once an access log exporter has been set-up, click on **Export Access logs** and you are presented with a window showing the destination of the file. Enter a file name with its extension and click on **Save**.

The following is an example of Exported Access logs.



Reports

The reports center has a variety of reporting options for displaying information about user activity.

List Report: Displays a list of all items in the selected category (Biometric Device, Operators and Users)

User Policy Members Report: Displays a list of all users that are members of the selected user policy.

Activity Reports: These reports will show all activity for the selected item type.

User Activity Report

- Select the desired date range. The default **Date Range** date and time is one week previous.
- Select the User. Enter the first few characters of both the first and last name. Select Search. Once the user is on the screen, select the user and click **Generate Report.**

© Refer to End User License Agreement for Copyright Notice

Biometric Device Activity Report

- Select the desired Date Range. The default **Date Range** date and time is one week previous.
- Select the Biometric Device. Enter the first few characters of the name of the Biometric Device. Select Search. Once the Biometric Device is on the screen, select the Biometric Device and click **Generate Report.** If you are not sure of the name or spelling of the Biometric Device, click on **Search** with an empty search box and all the Biometric Device will appear.

User Policy Activity Report

- Select the desired Date Range. The default **Date Range** date and time is one week previous.
- Select the User Policy. Enter the first few characters of the name of the policy. Select Search. Once the policy is on the screen, select it and click **Generate Report.** If you are not sure of the name or spelling of the policy, click on **Search** with an empty search box and all the user policies will appear.

All Activity (included all users and Biometric Device).

- Select the desired Date Range. The default **Date Range** date and time is one week previous.
- Click **Generate Report.**

Inactivity Report

- Select the desired Date Range. The default **Date Range** is one week previous.
- Select the User Group. Enter the first few characters of the name of the group. Select Search. Once the group is on the screen, select the group and click **Generate Report.**

List Report

- Select the Report type from the options Biometric Device, Operator, User and User group.
- Click **Generate Report.**

User Policy Members Report

- Search and select the User Policy and click on **Generate Report.**

Permissible Report

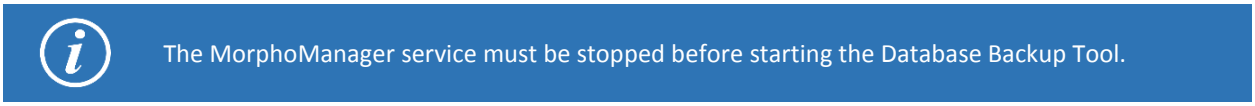
- Select the Report type (Biometric Device or User).
- Search for the Biometric Device name or the user name and click on **Generate Report.**

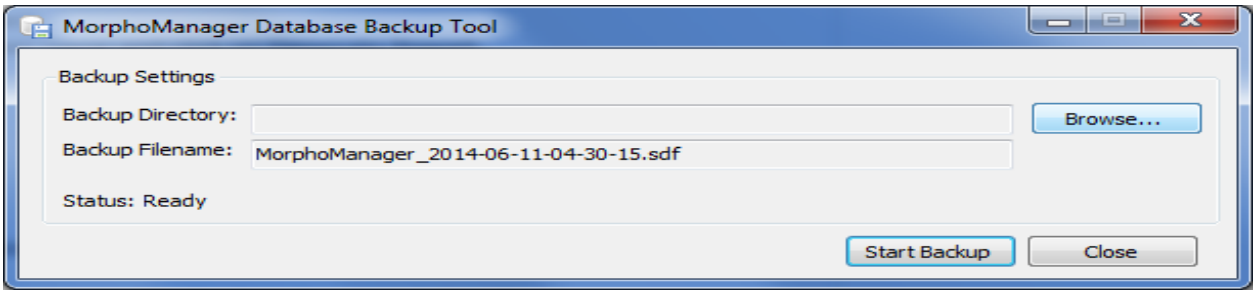
© Refer to End User License Agreement for Copyright Notice

Database Management

Database Backup Tool

The Backup Tool allows for the backup of SQLCE database. Systems running SQL Server will need to contact Microsoft for backup information.
When you start the Database Backup Tool, you will be prompted for backup directory. Select the directory you want to back up the database to.





Browse
Click Browse to change the backup directory

Start Backup
Starts the backup process.

Database Copy Tool

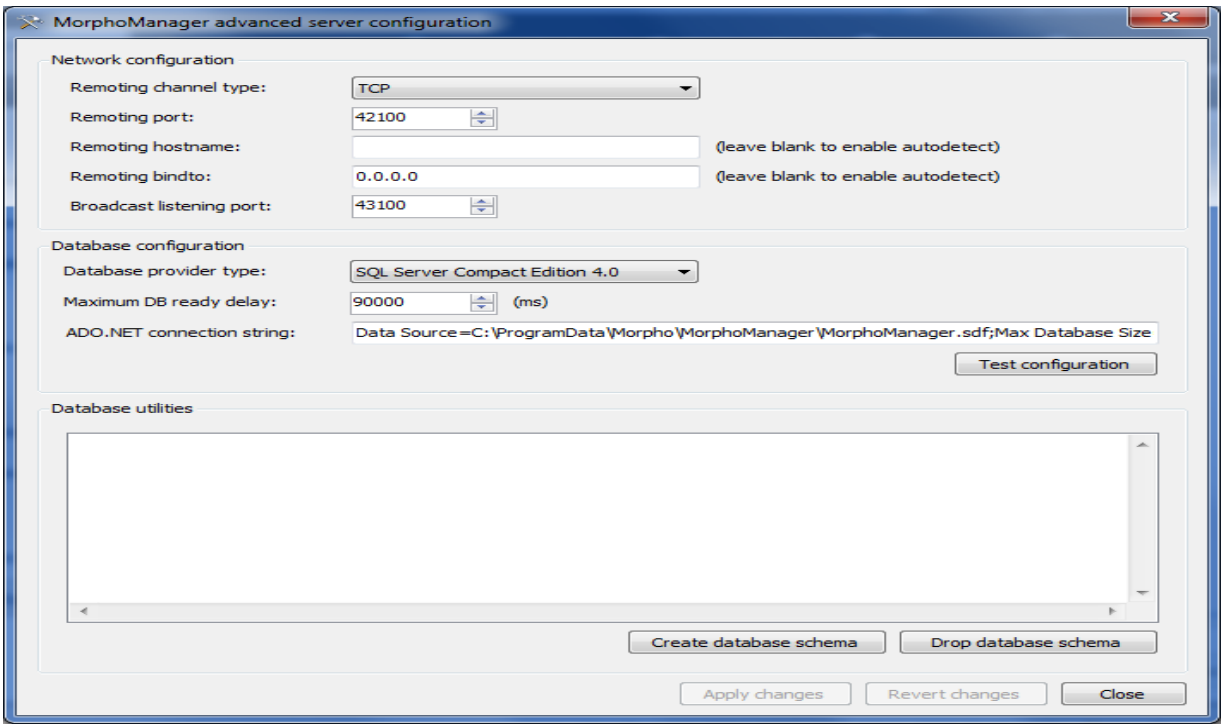
The Database Copy Tool copies a databases table schema and data from one database to another. This allows for easy upgrading from the default SQL CE database to Microsoft SQL server when the system grows beyond the limits of SQL CE.
For customer support on Microsoft SQL Server, please contact Microsoft SQL Server TechCenter.

Copying a database

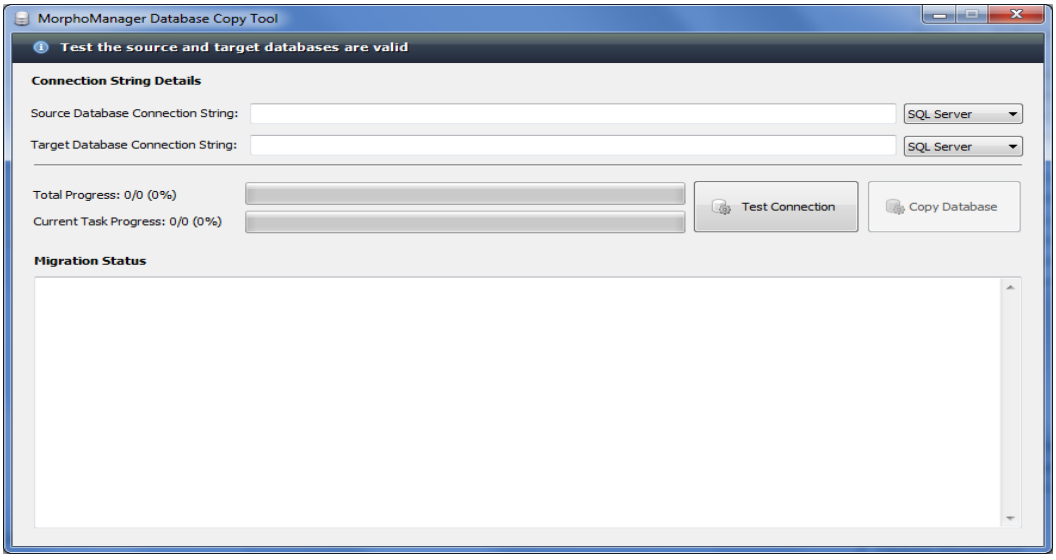
The following instructions are for upgrading the default SQL CE database to Microsoft SQL Server.

- **BACKUP YOUR CURRENT DATABASE.**
- Install and configure Microsoft SQL Server.
- Create a new database (MorphoManager)
- Stop MorphoManager Server
- Start Advanced server configuration

© Refer to End User License Agreement for Copyright Notice

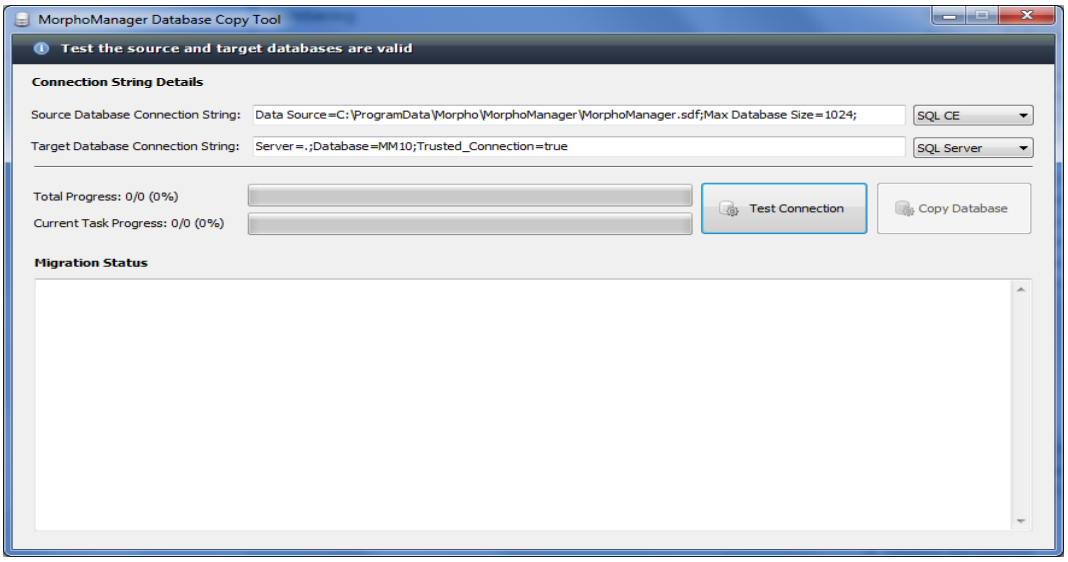


- Set Database provider type to SQL Server (200 and 2005)
- Set the ADO.Net connection string for the database you created. Save the existing ADO.NET connection string for later use.
- Apply changes
- Test configuration
- Create the database schema in the new database
- Start Database Copy Tool
- Connect String Details



© Refer to End User License Agreement for Copyright Notice

- Enter the ADO.NET connection string saved from 5.2 into the Source Database Connection String field.
- Set the correct database type using the dropdown lists.
- Test Connections
- Copy Database



- Verify your source and target database connection strings
- Click **Copy Database button**

All data within the target database will be erased.

Review the migration status to ensure no errors were encountered.

© Refer to End User License Agreement for Copyright Notice

Biometric Device Setup

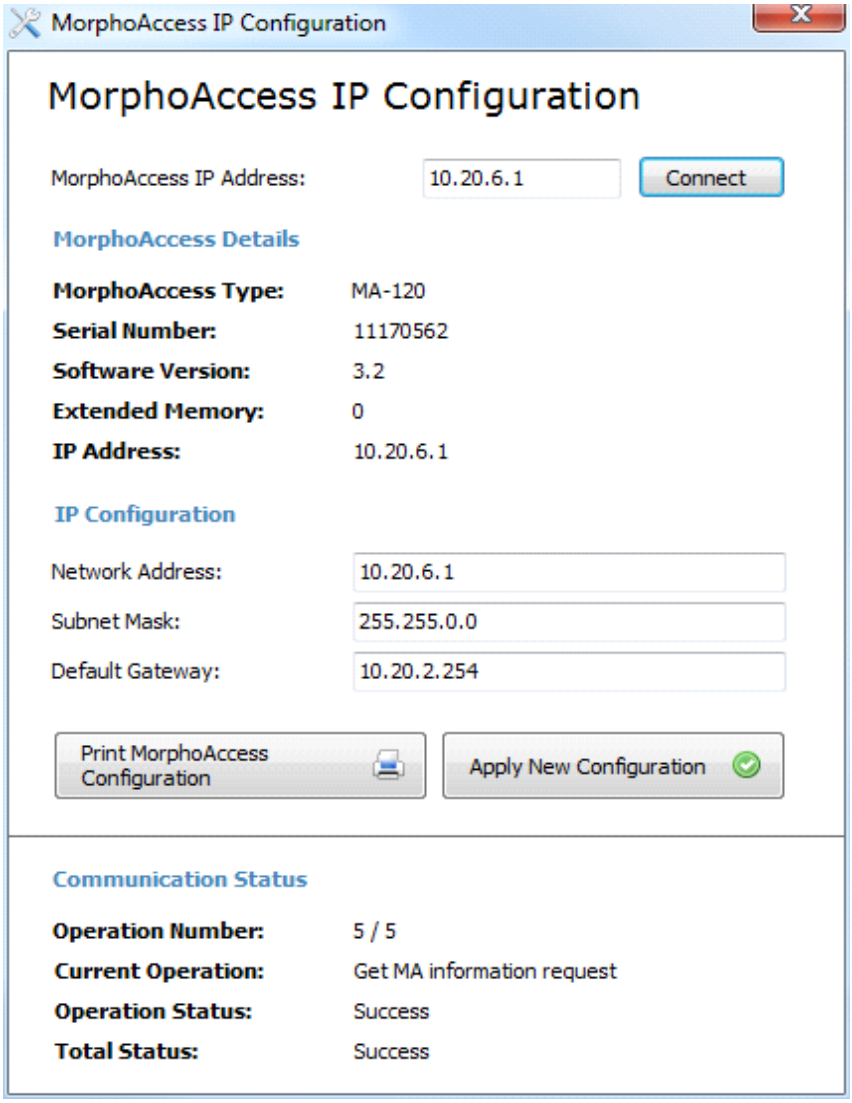
Biometric Device IP Address Configuration

By default all Biometric Device shipped from Safran are set to a default configuration.

IP Address: 134.1.32.214
Subnet Mask: 255.255.0.0
Default Route: 134.1.6.1

Use the Biometric Device IP Address Configuration Tool to change it.

The tool is located on the server installation in the program files menu.



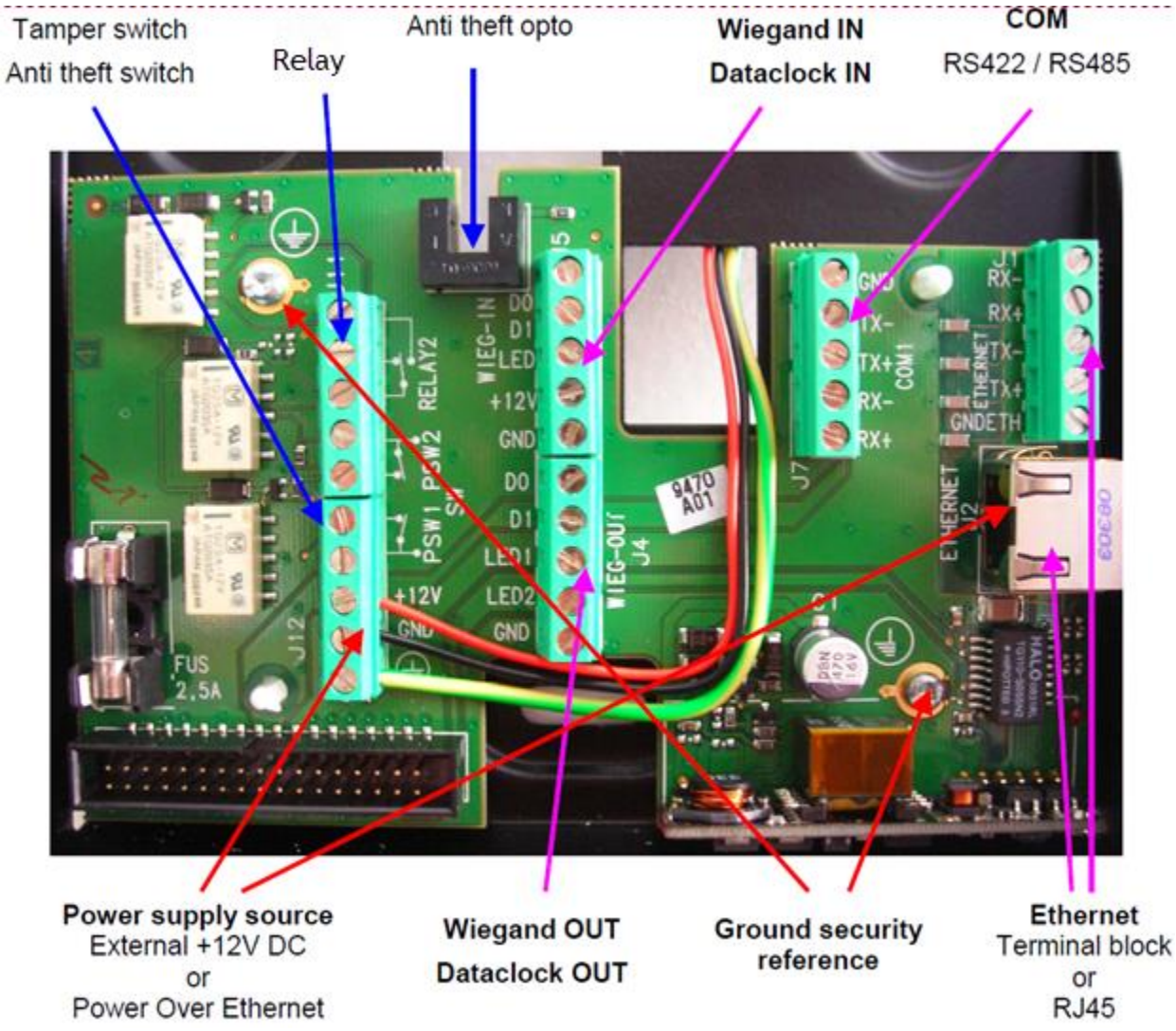
© Refer to End User License Agreement for Copyright Notice

Enter the existing IP address of the Biometric Device and click **Connect**.

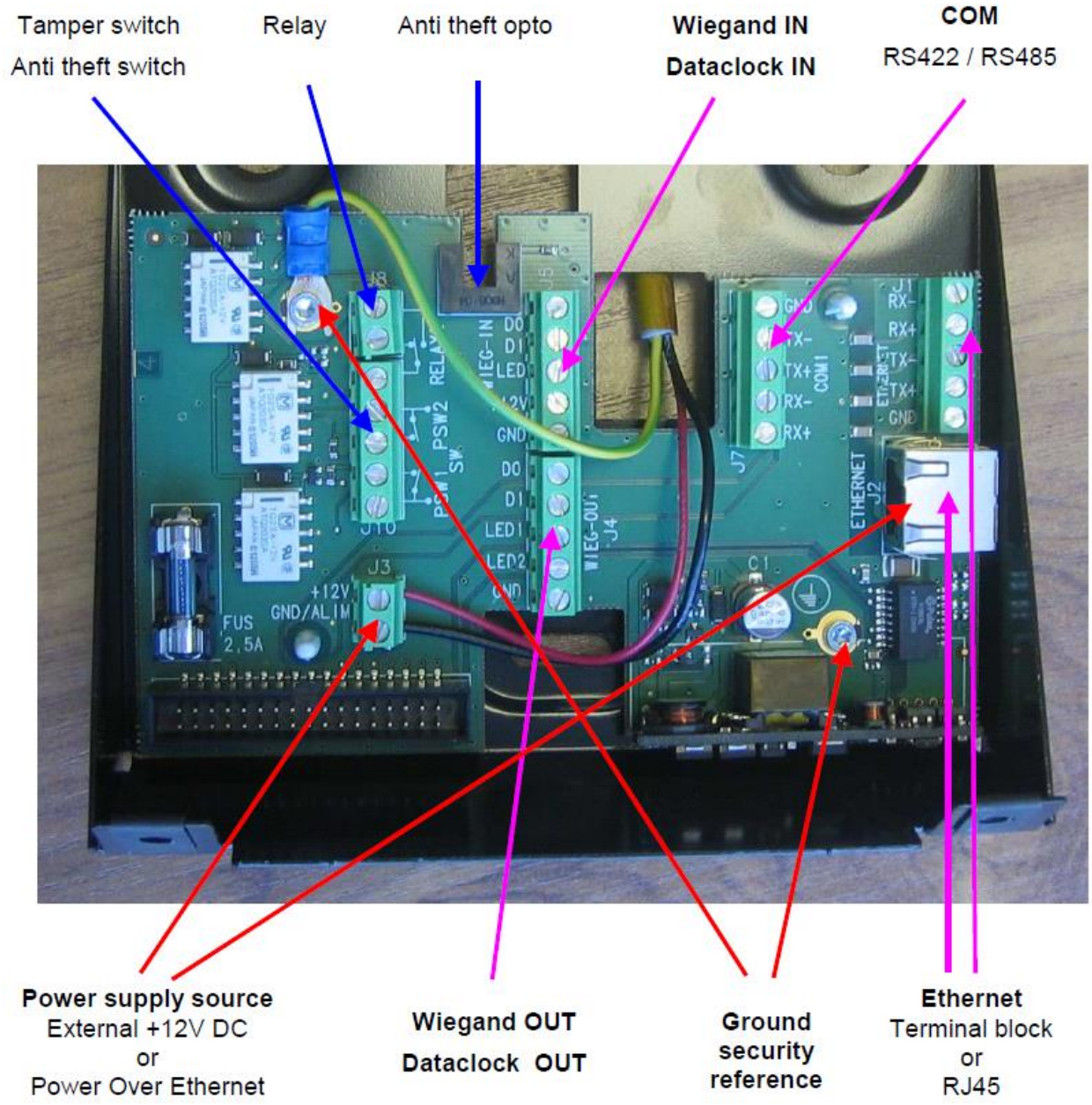
Enter the new configuration and click **Apply New Configuration**.

Biometric Device Wiring

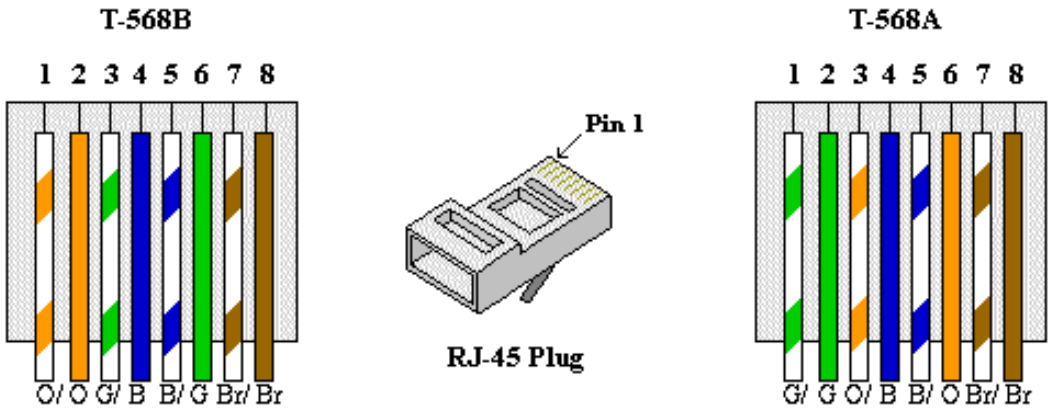
MA 500 / MA 500+ Series: New Block board wiring



MA 500 Series: Old block board wiring

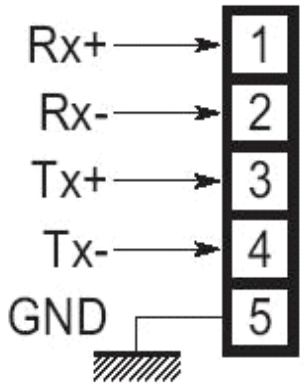


Ethernet Interface (LAN 10 Mbps)



T568B and T568A RJ45 Wire Positions

Pin	Signal	T568B Connection	T568A Connection
1	Tx (+) (Transmit Data +)	White Orange	White Green
2	Tx (-) (Transmit Data -)	Orange	Green
3	Rx (+) (Receive Data +)	White Green	White Orange
4	No Connection	Blue	Blue
5	No Connection	White Blue	White Blue
6	Rx (-) (Receive Data -)	Green	Orange
7	No Connection	White Brown	White Brown
8	No Connection	Brown	Brown



© Refer to End User License Agreement for Copyright Notice

Biometric Device TCP\IP Ethernet Wiring

Create a straight-through connection when connecting the Biometric Device into a Hub/Switch

Create a cross-over connection when connecting the Biometric Device directly into a computer.

RJ45 Wire Positions	Biometric Device Wiring	Result
T568B	T568B	Straight-through
T568B	T568A	Cross-over
T568A	T568A	Straight-through
T568A	T568B	Cross-over

For a straight-through connection match the T568B RJ45 Wire Positions to the T568B Biometric Device TCP\IP Ethernet Wiring.

For a cross-over connection, match the T568A RJ45 Wire Positions to the T568B Biometric Device TCP\IP Ethernet Wiring.

For a straight-through connection match the T568A RJ45 Wire Positions to the T568A Biometric Device TCP\IP Ethernet Wiring.

For a cross-over connection, match the T568A RJ45 Wire Positions to the T568B Biometric Device TCP\IP Ethernet Wiring.

Power Supply source

			MA 500 / MA 500+ Series OMA	500 Series
				Power Cable
1	+12V	In	Positive 12 Volts, power supply	Red
2	GND/ALIM	In	Ground power supply	Black
	Ground	In	Ground security reference	Yellow/green

External power supply: Must conform to CEE/EEC EN60950 standard 9V to 16 Volts ± 5% (regulated) 1.5 Amp minimum (peak) Power may come from a 12Volt Wiegand power supply, conforming to the Security Industry Association's Wiegand standard March 1995, able to deliver 9 Watts.

In standard operating activity, typical power consumption is 4.5 Watts. In extreme temperature conditions, with all options (USB Flash drive, 12V output for Wiegand in), maximum power consumption is up to 9 Watts. These Biometric Device make use of POE functionality; if Ethernet network is POE compatible, power supply may come from Ethernet wiring.

© Refer to End User License Agreement for Copyright Notice

Wiegand output wiring

			MA 500 / MA 500+ Series	OMA 500 Series
				Wiegand Dataclock cable
1	D0	Out	Wiegand D0	Green
2	D1	Out	Wiegand D1	White
3	LED1	In	Wiegand LED In 1 (Option)	Brown
4	LED2	In	Wiegand LED In 2 (Option)	Gray
5	GND		Ground for Wiegand	Black

Wiegand input wiring

			MA 500 / MA 500+ Series	OMA 500 Series
				Wiegand
1	D0	In	Wiegand D0	Blue
2	D1	In	Wiegand D1	Yellow
3	LED	Out	Wiegand LED Out 1 (Option)	Orange
4	+12V	Out	12 Volts Power output (150mA max)	Red
5	GND		Ground for Wiegand	Black

Output relay and Tamper-Switch

		MA 500 / MA 500+ Series	OMA 500 Series
			Switch/relay cable
1	CRO	Contact relay normally open	Red
2	CRC	Contact relay normally closed	Orange
3	CR	Contact relay common	Yellow
4	TSW2_1	Tamper switch Contact 1	White
5	TSW2-0	Tamper switch Contact 0	Green
6	ATSW1_1	Anti theft switch Contact 1	Not available
7	ASTW1_0	Anti-theft switch Contact 0	Not available
	Ground	Not connected	Black

© Refer to End User License Agreement for Copyright Notice